Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra obchodu a financí

Diplomová práce

Obchod a bezhotovostní platební instrumenty

Bc. Aleš Podaný

© 2017 ČZU v Praze

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Aleš Podaný

Veřejná správa a regionální rozvoj

Název práce

Obchod a bezhotovostní platební instrumenty

Název anglicky

Business and Cashless Payment Instruments

Cíle práce

Hlavním cílem práce bude identifikovat aktuální možná rizika při realizaci bezhotovostního způsobu placení u obchodníka a návrh optimálních opatření, která zajistí vyšší úroveň bezpečnosti. Dílčím cílem bude vyhodnocení trendu důvěry klientů finančních institucí a obchodníků v nástroje bezhotovostního platebního styku na základě provedení dotazníkového šetření a jeho statistického vyhodnocení.

Metodika

Metodika zpracování teoretických východisek bude zaměřena na studium odborné literatury, norem, článků a dalších dokumentů tištěného i digitálního charakteru. Na základě studia zkoumaného jevu budou vybrána adekvátní teoretická

východiska, která budou užitá při zpracování práce.

Vlastní práce bude vycházet z charakteristiky konkrétních bezhotovostních platebních nástrojů a popisu současného stavu a trendu vývoje zkoumané problematiky na základě odborných dokumentů, materiálů bank a ostatních finančních institucí poskytujících služby platebního styku. K identifikaci konkrétních rizik a možných návrhů vylepšení platebních postupů z hlediska zvýšení bezpečnosti a komfortu bude použita metoda komparaces teoretickými východisky, metoda analýzy a syntézy zjištěných skutečností a empirické metody poznání s využitím dotazníkového šetření, jeho statistického vyhodnocení a závěrů. Zjištěné skutečnosti budou zpracovány pomocí programů Microsoft World a Microsoft Excel.

Doporučený rozsah práce

60 – 80 stran

Klíčová slova

Bezhotovostní styk, instrument, obchod, zúčtování, platební podmínka.

Doporučené zdroje informací

JIRKŮVOVÁ, Margita; MAREK, Karel; TOMÍČKOVÁ Silvie. Banky, bankovní služby, burza. Brno: Iuridica Brunensia, 1995. 242 s. ISBN 80-85964-09-0.

JUŘÍK, Pavel. Platební karty Velká encyklopedie 1870-2006. 1. vyd. Praha: Grada, 2006. 296 s. ISBN 80-247-1381-0.

LUK, K W. *International trade finance : a practical guide.* Hong Kong: City University of Hong Kong Press, 2011. ISBN 978-962-937-185-2.

MÁČE, Miroslav. Platební styk. 1. vyd. Praha: Grada, 2006. 220 s. ISBN 80-247-1725-5.

PŘÁDKA, Michal; KALA, Jan. Elektronické bankovnictví. Praha: Computer Press, 2000. 178 s. ISBN 80-7226-328-5.

REUVID, J. – SHERLOCK, J. *International trade : an essential guide to the principles and practice of export.* London: Kogan Page, 2011. ISBN 978-0-7494-6237-6.

SATO, A. – MACHKOVÁ, H. – ČERNOHLÁVKOVÁ, E. *Mezinárodní obchodní operace.* Praha: Grada, 2007. ISBN 978-80-247-1590-2.

SCHLOSSBERGER, Otakar. Platební služby. 1. vyd. Praha: Management Press, 2012. 325 s. ISBN 978-80-7261-238-3.

Předběžný termín obhajoby

2016/17 LS – PEF

Vedoucí práce

Ing. Olga Regnerová

Garantující pracoviště

Katedra obchodu a financí

Elektronicky schváleno dne 8. 11. 2016

Ing. Helena Čermáková, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 9. 11. 2016

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 13. 03. 2017

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Obchod a bezhotovostní platební instrumenty" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 22. března 2017 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Olze Regnerové za odbornou pomoc a cenné připomínky během zpracovávání mé diplomové práce.

Obchod a bezhotovostní platební instrumenty

Souhrn

Tématem diplomové práce je vyhodnocení bezhotovostních platebních nástrojů, se zaměřením na platební karty a internetové bankovnictví. Práce vyhodnocuje jednotlivé funkční prvky vybraných platebních nástrojů, se zaměřením na zajištění jejich bezpečnosti. První část práce se zabývá využíváním vybraných platebních nástrojů klienty, dodržováním základních bezpečnostních zásad nebo doporučení bank, a to formou dotazníkového šetření. Na základě vyhodnocení odpovědí respondentů jsou formulovány závěry, které vycházejí z jejich praktických zkušeností. Druhá část práce je věnována aktuálním rizikům, která mohou ohrozit peněžní prostředky, při využívání bezhotovostního způsobu placení. Ve třetí části je provedena komparace vybraných aplikací internetového bankovnictví, se zaměřením na porovnání bezpečnostních prvků a nalezení možných vylepšení. Tématem čtvrté části práce je šetření, v jaké míře je využíván bezpečnostní kryt PINpadu platebního terminálu, který významně snižuje riziko odpozorování PINu platební karty. S využitím pozorování, učiněných v náhodně vybraných obchodech je statisticky vyhodnocena míra využití tohoto bezpečnostního prvku a následně kvantifikována míra rizika úspěšného odpozorování PINu. Aktuální bezpečnostní situaci v oblasti platebních karet v České republice, měřeno počtem vydaných platebních karet, četností a objemem transakcí a počtem případů podvodného jednání, nalezneme v poslední části práce.

Klíčová slova: Platební karta, platební styk, bankovnictví, bezhotovostní, autorizace, autentizace, bankomat

Business and Cashless Payment Instruments

Summary

The topic of my dissertation is evaluation of cashless payment instruments with concentrating on cash cards and internet banking. My dissertation evaluates individual functional components of select payment instruments with concentrating on to their safety. The first part of my dissertation take an interest in utilization selected payment instruments of the clients, by keeping the first safety principles or recommendation of the banks by the form of questionnaire. The conclusions are formulated on the basis of answers of respondents which came from their experiences. The second part of my work is given to actual risks they can jeopardize financial funds by utilization of cashless payment. In the third part of my work is made comparison with selected application of internet banking with concentrating of comparison safety elements and trying to find improving of them. The forth part of my dissertation is investigation how much is using the safety cover of PINpad payment terminal which take less risk by watching PIN of cash card. There was taken an observation in some shops and than was statistically evaluated extend for using this safety element and than quantified the risk of steal the PIN. In the last part of my dissertation we can find the actual safety situation in the sphere of cash cards in the Czech republic. It means it is measured by edition of cash cards their frequent and extend of transaction and by the cases of frauds.

Keywords: Payment card, payments, banking, cashless, authorization, authentication, automated teller machine

Obsah

Seznam obrázků

Seznam grafů

Seznam tabulek

Použité zkratky

CERTIS	Systém mezibankovního platebního styku
ČNB	Česká národní banka
ČR	Česká republika
EMV	Europay/MasterCard, VISA
PČR	Policie České republiky
PIN	Osobní identifikační číslo
POS	Platební terminál
SBK	Sdružení pro bankovní karty

1 Úvod

Tématem diplomové práce je obchod a bezhotovostní platební instrumenty. Důvodem pro výběr tohoto tématu, byla jeho zajímavost a praktické využití výstupů pro širokou veřejnost.

Každá realizace obchodu v rámci vyspělého trhu má možnost využití rozmanitých instrumentů platebního styku. Při provádění plateb je kladen důraz na komfort, efektivitu a bezpečnost. To znamená jednoduchost platební operace, co nejnižší transakční náklady, a zajištění bezpečnosti finančního majetku.

V širším vymezení je platební styk definovaný jako systém provozovaný bankami a ostatními finančními institucemi, prostřednictvím kterého jsou realizovány finanční převody mezi jednotlivými hospodářskými subjekty, kterými jsou jak fyzické tak právnické osoby. Převod finančních prostředků je realizován pomocí různých platebních instrumentů. Předmětem této práce jsou nástroje, umožňující bezhotovostní platby a to jak z pohledu jejich funkčnosti, tak z pohledu zabezpečení ochrany finančních převodů.

Bezhotovostní platební styk umožňuje zabezpečené a pohodlné platby. Bezesporu lze konstatovat, že bezhotovostní platby, oproti hotovostnímu platebnímu styku, mají, mimo jiné výhody, zpravidla nižší transakční náklady. V rámci ekonomické racionality je tak pro lidi výhodný přechod na platby v jejich elektronické podobě.

Dalším významným faktorem, který ovlivňuje používání bezhotovostního platebního styku je důvěra klientů v bezhotovostní instrumenty, která je dána úrovní zabezpečení těchto instrumentů finančními institucemi, poskytujících služby platebního styku. Důležitá je zejména včasná reakce bank a ostatních finančních institucí na podvodná jednání, která předchází dalším ztrátám a minimalizuje rizika svých klientů.

Dalším významným faktorem, ve prospěch bezhotovostních peněz je zjednodušení platebních postupů s využitím technologických inovací. Díky vývoji v oboru informačních technologií, ke kterému došlo v předešlých dvou desetiletích a v návaznosti i právní úpravě platebního styku, kterou si technologický pokrok vynutil, došlo k zavedení nových

platebních instrumentů, jako například elektronické peněženy nebo mobilních platebních prostředků. Tyto nové platební instrumenty umožnily zjednodušení placení u obchodníka, a zavedení nových služeb, které zvýšili jejich atraktivitu.

V České republice je prostor pro růst poměru bezhotovostního způsobu plateb u obchodníků stále veliký. V klíčových ukazatelích bezhotovostního platebního styku, i přes výrazný pokrok, za vyspělými trhy stále zaostáváme.

Mezi faktory brzdící rozvoj trhu bezhotovostních instrumentů je nedostatečná vybavenost obchodníků platebními terminály. Tento potenciál je potřeba rozumně využít, což se zejména neobejde bez investic do infrastruktury platebních systémů.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem práce je identifikace aktuálních možných rizik při realizaci bezhotovostního způsobu placení u obchodníka a návrh optimálních opatření, která zajistí vyšší úroveň bezpečnosti bezhotovostního obchodování při zachování, nebo zvýšení současného stavu komfortu a jednoduchosti jednotlivých platebních instrumentů.

Podpůrným cílem je zachycení trendu důvěry klientů finančních institucí a obchodníků v nástroje bezhotovostního platebního styku, provedení dotazníkového šetření a jeho statistické vyhodnocení.

2.2 Metodika

Metodika zpracování teoretických východisek bude zaměřena na studium odborné literatury, norem, článků a dalších dokumentů tištěného i digitálního charakteru. Analýza dat, komparace a deskripce. Na základě studia zkoumaného jevu budou vybrána adekvátní teoretická východiska, která budou užitá při zpracování práce. Vlastní práce bude vycházet z charakteristiky konkrétních bezhotovostních platebních nástrojů a popisu současného stavu a trendu vývoje zkoumané problematiky na základě odborných dokumentů, materiálů bank a ostatních finančních institucí poskytujících služby platebního styku. K identifikaci konkrétních rizik a možných návrhů vylepšení platebních postupů z hlediska zvýšení bezpečnosti a komfortu bude použita metoda komparace s teoretickými východisky, metoda analýzy a syntézy zjištěných skutečností a empirické metody poznání s využitím dotazníkového šetření, jeho statistického vyhodnocení a závěrů. Zjištěné skutečnosti budou zpracovány pomocí programů Microsoft World a Microsoft Excel.

Za účelem sběru dat v dotazníkovém šetření, bude s využitím programu Microsoft World vyhotoven dotazníkový formulář. Dotazníkový formulář bude vyhotoven jak v analogové, tak i v elektronické podobě. Respondenti budou pro účely hlubší analýzy rozděleni podle pohlaví, věku nebo vzdělání. Dotazníkové šetření bude rozděleno do tří tematických okruhů. První tematický okruh bude zaměřen na používání elektronického

bankovnictví, druhý tematický okruh na používání platebních karet a třetí tematický okruh bude zaměřen na chování a dodržování základních bezpečnostních zásad respondenty. Nasbíraná data budou zpracována v programu Mocrosoft Excel, ve kterém budou zpracována v podobě statistických tabulek a grafů, prostřednictví kterých budou vyhodnoceny zjištěné skutečnosti a formulovány závěry a výsledky dotazníkového šetření.

Pro vyhodnocení bezpečnosti internetového bankovnictví bude provedena komparace čtyř vybraných služeb internetového bankovnictví. Sledována budou kritéria přihlášení do aplikace bankovnictví, provádění transakcí, zabezpečení komunikace, poskytování informací a bezpečnostní politika banky. Zdrojem bude studium materiálů a informací bank a vlastní zadáváni platebních příkazů prostřednictvím aplikace internetového bankovnictví hodnocených bank.

V rámci šetření, s využitím empirické metody pozorování, bude proveden průzkum, v rámci kterého bude sledováno, v jaké míře je aktuálně v obchodech využíván bezpečnostní prvek, kryt PINpadu platebního terminálu. Rozsah a reprezentativnost sledovaného souboru bude vybrán tak, aby bylo dosaženo sledovaného cíle na dostatečné úrovni. Pro vyhodnocení šetření bude v programu Excel zpracována statistická tabulka a vizualizace v podobě grafů. Pro výpočet výše rizika úspěšného odpozorování PINu platební karty bude použit vzorec, který je tvořen sumou podílů ochodů násobených rizikem odpozorování, podle vybavenosti krytem PINpadu platebního terminálu, vycházející ze zjištění konkrétních rizik odpozorování v experimentu provedeném v letech 2005 a 2006 na Fakultě informatiky Masarykovi univerzity.

Další řešenou oblastí je současná situace bezpečnosti platebních karet. Za tímto účelem budou zjištěny statistiky kriminality, vedené policií České republiky a statistiky platebních karet, vedené Sdružením pro bankovní karty. Bude vyhotovena vlastní statistická tabulka, s využitím programu Mocrosoft Excel. Pro analýzu vývoje a trendů budou data sledována v určitém období, a to let 2011 až 2015.

3 Teoretická východiska

3.1 Vymezení základních pojmů

Platební prostředek

Ve smyslu ustanovení § 2 odst. 1 písm. d) zákona č. 284/2009 Sb., o platebním styku, ve znění pozdějších předpisů (dále jen „zákon o platebním styku“), se rozumí platebním prostředkem zařízení nebo soubor postupů dohodnutých mezi poskytovatelem a uživatelem, které jsou vztaženy k osobě uživatele a kterými uživatel dává platební příkaz (Zákon č. 284/2009 Sb., o platebním styku, ve znění pozdějších předpisů).

Platební systém

Platebním systémem se rozumí systém, který zajišťuje převody peněz mezi subjekty platebního systému.

Platební účet

Je definován zákonem o platebním styku, kdy se platebním účtem rozumí účet, který slouží k provádění platebních transakcí. Pravidla tvorby čísla účtu v platebním styku jsou stanoveny vyhláškou ČNB č. 169/2011 Sb., o stanovení pravidel tvorby čísla účtu v platebním styku, ve znění pozdějších předpisů.

Platba

Pojmem platba se rozumí převod peněz z účtu plátce na účet příjemce platby, realizovaný platebním prostředkem.

Autentizace uživatele

Autentizace uživatele je pojem představující proces, při kterém se ověřuje identita uživatele, který vstupuje do systému. V rámci tohoto procesu dochází k jednoznačnému určení identity uživatele.

Autorizace uživatele

Proces autorizace uživatele zpravidla navazuje na proces autentizace uživatele, jedná se o ověření oprávnění provést příslušnou akci.

Autorizace platební transakce

Termínem autorizace platební transakce je myšleno, jak ověřování identity uživatele a jeho oprávnění, tak i kontrola dat spojených s transakcí a finančního krytí.

3.2 Základní přehled právní úplavy platebního styku

Platební styk je často chápán pouze jako prosté placení prostřednictvím bank bez hlubší znalosti jeho jednotlivých forem a instrumentů. Ty se od sebe někdy podstatně liší a vycházejí z různých pramenů práva (Máče, 2006).

Vzhledem k tomu, jak širokou oblastí je platební styk, není možné upravit jeho právní rámec jedinou právní normou. Je tomu tak i proto, že jako na každou činnost podniku nebo banky, i na platební styk se vztahují obecné právní normy, současně je ovšem nutné, aby detailní provádění operací v platebním styku bylo upraveno specializovanými normami, ať už jde o normy s nejvyšší účinností (zákony) nebo o normy prováděcí v podobě vyhlášek (Polouček a kol., 2006).

Platby jsou v České republice považovány za soukromoprávní vztah a jsou v obecné rovině podřízeny občanskému zákoníku. Tento kodex obsahuje též základní principy bankovních obchodů, o které se opírají vztahy mezi bankou a klientem. (Jílek, 2013)

Právní předpisy vztahující se k úpravě platebního styku lze dle údajů České národní banky rozdělit do tří skupin:

1. Předpisy EU,
2. zákony,
3. vyhlášky,

3.2.1 Předpisy Evropské unie

Právní úprava platebního styku na úrovni Evropské unie (EU) je nejčastěji řešena právními akty ve formě nařízení nebo směrnice. Zatímco Nařízení Evropského parlamentu a Rady jsou pro členský stát Evropské unie závazná a přímo použitelná, tak Směrnice

Evropského parlamentu a Rady určují dosažení konkrétního cíle a vyžadují implementaci do právního řádu členského státu, tedy i právního řádu České republiky.

Stěžejní právní normou upravující platební styk na úrovni Evropské unie je směrnice 98/26/ES Evropského Parlamentu a Rady ze dne 19. května 1998 o neodvolatelnosti zúčtování v platebních systémech a v systémech vypořádání obchodů s cennými papíry, ve znění pozdějších předpisů.

Dalšími předpisy Evropské unie upravujícími oblast platebního styku jsou například směrnice 2006/48/ES Evropského parlamentu a Rady ze dne 14. června 2006 o přístupu k činnosti úvěrových institucí a o jejím výkonu, ve znění pozdějších předpisů, směrnice 2007/64/ES Evropského parlamentu a Rady ze dne 13. listopadu 2007 o platebních službách na vnitřním trhu, ve znění pozdějších předpisů, nařízení 1781/2006/ES Evropského parlamentu a Rady ze dne 15. listopadu 2006 o informacích o plátci doprovázejících převody prostředků, ve znění pozdějších předpisů, atd. (Jílek, 2013).

3.2.2 **Zákony**

Zákon č. 284/2009 Sb., o platebním styku, ve znění pozdějších předpisů, (dále jen „zákon o platebním styku“). Zákon o platebním styku je základní právní normou upravující platební styk na území České republiky. Lze ho rozdělit na veřejnoprávní a soukromoprávní část. Ve veřejnoprávní části jsou mimo jiné stanoveny podmínky pro získání povolení podnikat jako poskytovatel platebních služeb, dále zde nalezneme úpravu postavení platebního systému a podmínky pro jeho fungování. Soukromoprávní část je zaměřena na podmínky poskytování platebních služeb, se zaměřením na práva a povinnosti poskytovatelů vůdči uživatelům těchto služeb (Schlossberger, 2012).

Zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, (dále jen „zákon o bankách“). Zákon o bankách zapracovává do právního řádu České republiky příslušné předpisy Evropské unie, především směrnici 94/19/ES Evropského parlamentu a Rady ze dne 30. května 1994 o systémech pojištění vkladů, ve znění pozdějších předpisů a nařízení 575/2013 Evropského parlamentu a Rady ze dne 26. června 2013, o obezřetnostních požadavcích na úvěrové instituce a investiční podniky, ve znění pozdějších předpisů.

Upravuje některé vztahy související se vznikem, provozováním bank a jejich zánikem. Činnost banky, jako poskytovatele platebních služeb je vymezena v ustanovení § 1 odst. 3 písm. c)zákona o bankách (zákon č. 21/1992 Sb.).

Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů, ve znění pozdějších předpisů, který stanovuje povinnosti ČNB při přípravě na krizové situace, především v oblasti měnové politiky a bankovnictví (ČNB).

3.2.3 **Vyhlášky**

Vyhláška č. 169/2011 Sb., ze dne 7. června 2011, o stanovení pravidel tvorby čísla účtu v platebním styku, která upravuje pravidla tvorby čísla účtu v souladu s mezinárodní standardizací vymezenými normou ISO 13616.

Vyhláška č. 140/2011 Sb., ze dne 12. května 2011, o platebních systémech s neodvolatelností zúčtování, která především vymezuje náležitosti žádosti o povolení k provozování platebního systému a vymezuje některé pojmy.

Vyhláška č. 141/2011 Sb., ze dne 13. května 2011, o výkonu činnosti platebních institucí, institucí elektronických peněz, poskytovatelů platebních služeb malého rozsahu a vydavatelů elektronických peněz malého rozsahu, která zejména vymezuje náležitosti žádosti o povolení k činnosti platební instituce, žádosti o zápis do registru poskytovatelů platebních služeb malého rozsahu, žádosti o povolení k činnosti instituce elektronických peněz a vymezuje některé pojmy (ČNB).

V rámci platné právní úpravy platebního styku v České republice, která vychází z mezinárodních dohod a legislativy Evropské unie která je implementována do právního rámce České republiky, se finanční instituce snaží o maximalizaci prováděných platebních transakcí na úkor maximalizace bezpečnosti. Maximální míru odpovědnosti za provedené finanční transakce, pokud jim to legislativa umožňuje, přesouvají na zákazníka. Bezpečnostní prvky jim usnadňují dokazování zavinění zákazníka a chrání zejména zájmy bank a obchodníků (Matyáš, Krhovják a kol., 2008).

3.3 Platební systémy

3.3.1 Platby

Lidé se vždy snažili najít co nejpohodlnější, nejbezpečnější, nejspolehlivější a nejlevnější způsob placení. Moderní elektronické platební nástroje a elektronické peníze snížily náklady na hotovostní oběh, hrazené finančními institucemi, obchodníky zákazníky. I přes dominantní postavení hotovostního způsobu plateb v maloobchodní síti má bezhotovostní placení rostoucí tendenci a stále více vytlačuje hotovost (Juřík, 2012).

Bezhotovostní platby u obchodníka jsou realizovány prostřednictvím bank a ostatních finančních institucí, které poskytují služby platebního styku. Realizace plateb je zajištěna souborem finančních operací a instrumentů elektronického bankovnictví. Tato činnost finančních institucí, která vstupuje mezi obchodníka a zákazníka, poskytuje službu elektronickou formou, jejímž úkolem jsou debetní a kreditní operace na účtech svých klientů (Máče, 2006).

Kromě výnosu, která uložené peníze nesou, je důvodem pro založení účtu v bance i možnost provádět snazším způsobem platby. Většina vkladů umožňuje majitelům účtu platit šekem nebo používat platební kartu. Je to pohodlnější než platit hotovými penězi (Frank, Bernanke,2002).

Platby realizované prostřednictvím bank a ostatních finančních institucí tvoří ve vyspělých trzích podstatnou část plateb v ekonomice. Díky rozsáhlé a vzájemně propojené síti bank, s využitím informačních technologií banky nabízejí nové platební instrumenty, díky kterým jsou schopné provádět platby rychle a bezpečně téměř po celém světě (Revenda, Mandel, Kodera, Musílek, Dvořák, 2014).

Možnost mít čtyřiadvacet hodin přístup ke svému účtu je jednou z výhod služeb přímého bankovnictví, které klientovi umožňují obsluhu bankovních produktů na dálku. Tyto služby jsou poskytovány na smluvním základě, kdy jsou klientovy předány kódy a hesla, potřebné při využívání služeb přímého bankovnictví. Aby bylo možné zadokumentovat pokyny klienta je každý jeho kontakt s bankou zaznamenán (Kalabis, 2012).

Při placení u obchodníků jsou stále častěji jako platební prostředek používány platební karty. Každá operace s platební kartou musí být zajištěna proti jejímu zneužití. Toto zajištění bezpečnosti užívání platebních karet je neustále konfrontováno se snahou podvodníků obejít bezpečnostní prvky ochrany a neoprávněně získat finanční prostředky držitelů platebních karet (Polouček a kol.,2006).

Platební příkazy klienta bance, platby kartou a ostatní mezibankovní operace jsou zpracovány systémem mezibankovního zúčtování, kterým je v České republice systém mezibankovních plateb CERTIS (Czech express real time interbank gross settlement system). Provozovatelem tohoto systému je zúčtovacím centrem České národní banky. Finanční transakce jsou zpracovány a vypořádány, v průběhu tohoto procesu se mimo jiné provádí kontrola dostatku likvidity na účtu plátce a v případě dostatečného krytí je prováděna platba. Zúčtování je v digitální formě předáváno účastníkům prostřednictvím komunikační sítě (Jílek, 2013).

3.3.2 **Platební systémy**

Platební systém či systém převodu peněz nebo likvidity je systém, který zajišťuje převody peněz nebo likvidity. Může být provozován buď na principu zúčtování (clearing) a vypořádání jednotlivých položek při současné kontrole jejich krytí – **hrubý platební systém,** nebo na principu zúčtování rozdílů (sald) vypočtených ze vzájemných pohledávek a závazků účastníků systému – **čistý platební systém**, popřípadě jako kombinace těchto principů (Jílek, 2013).

Platební systémy jsou nezbytné, pro realizaci obchodních transakcí v každé moderní ekonomice. Struktura plateb se skládá z celé řady služeb zúčtování a vypořádání. Pokrok v informačních technologiích umožnil výrazný pokrok ve vývoji bankovní infrastruktury, prostřednictvím které je realizován bezhotovostní platební styk (Hartmann, 2000).

Z hlediska zúčtování samého, lze dle Schlossbergera, platební systémy rozdělit na **systém korespondentský** a **systém s clearingovou autoritou.**

Korespondentský platební systém je založen na vzájemných korespondentských vztazích účastníků a vedení korespondentských účtů tzv. nostro a loro účtů. V případě, kdy banka

potřebuje zúčtovat položku platebního styku do banky klienta, se kterým nemá přímé bankovní spojení, pak musí banka příkazce využít prostředníka – tzv. zprostředkující banku.

Claringový platební systém je takový, ve kterém jsou jednotliví členové platebního systému napojeni svým bankovním spojením, nostro účtem, na jednu zúčtovací autoritu, kterou bývá buď banka (velmi často centrální banka), nebo jiná k tomu určená právnická osoba bankovního typu (Schlossberger, 2012).

Použití zúčtovacích platebních systémů je typické pro vnitrostátní platební styk, respektive pro platební styk přeshraniční. Zákonná úprava, v podmínkách Evropské unie, upravuje nejen vnitřní strukturu a podmínky provozování těchto systémů, ale i povinnost použít pro platbu v určitém hospodářském prostoru i některý z platebních systémů v něm existujících (Polouček a kol.,2006).

V České republice je využíván platební systém CERTIS, v rámci kterého jsou veškeré mezibankovní platby v korunách na území České republiky zpracovávány zúčtovacím centrem České národní banky. Zúčtovacím centrem ČNB jsou zpracovávány jak transakce bank, tak jejich klientů. Za tímto účelem mají banky zřízen u ČNB účet mezibankovního platebního styku. Každý účastník systému se identifikuje kódem platebního styku, který je povinnou součástí každé transakce (Schlossberger, 2012).

Zpracování plateb

Zúčtování plateb zpravidla provádí banka, která obdrží od smluvních obchodníků účtenky nebo elektronické údaje o provedených platbách. Následně jsou data o provedených platbách bankou odeslána do zúčtovacího centra, kterým je v České republice ČNB. Zúčtovací centrum vytváří datové soubory pro banky, konverzuje měny atd.. Provede zúčtování a zašle bankám informace o jejich saldech, které je nutné vypořádat. Mezinárodní platební operace provádí příslušná kartová společnost (Jílek, 2013).

3.3.3 Poskytovatelé platebních služeb

Dle právní úpravy, která je obecně vymezena zákonem o platebním styku a v souladu se specifickou právní úpravou, jsou na území České republiky oprávněny poskytovat služby platebního styku tyto instituce:

- banky,
- zahraniční banky a zahraniční finanční instituce,
- spořitelní a úvěrní družstva,
- instituce elektronických peněz,
- zahraniční instituce elektronických peněz,
- vydavatelé elektronických peněz malého rozsahu,
- platební instituce,
- zahraniční platební instituce,
- poskytovatelé platebních služeb malého rozsahu,
- Česká národní banka

3.4 Instrumenty bezhotovostního platebního styku

Tato kapitola se bude zabývat vybranými nástroji bezhotovostního platebního styku, které jsou základními a nejpoužívanějšími prvky bezhotovostního platebního styku.

3.4.1 Běžný účet

Prostřednictvím nových komunikačních technologií, kterými jsou především mobilní či pevné linky nebo internet, se klient banky stává pánem svého času. Do komunikace se svou bankou může vstoupit kdykoliv a odkudkoliv, čímž odpadají zdlouhavé návštěvy poboček bank za účelem provádění běžných bankovních operací. Nové komunikační kanály poskytují nové možnosti, jako například možnost objednat a platit služby i zboží prostřednictvím internetu (Máče, 2006).

Všechny poskytované produkty a služby obchodních bank se vždy vážou k běžnému účtu klienta. V teorii i praxi se lze setkat s pojmem žirový účet, který má v různých bankách různý název (např. sporožiro v České spořitelně nebo expres konto v Komerční bance). Tento název jen zdůrazňuje, že jde vždy o formu běžného účtu ve smyslu současné právní úpravy, neboť účet je zejména určen pro bezhotovostní placení převodem peněžních prostředků z tohoto účtu (Schlossberger, Soldánová 2005).

Běžný účet – mohou zřizovat a vést banky tuzemcům i cizozemcům, jak právnickým tak i fyzickým osobám v korunách nebo v jakékoliv cizí měně. Slouží zejména k zajištění platebního styku tuzemského i zahraničního, k zúčtování všech operací z příkazu majitele účtu, osob zmocněných majitelem účtu nebo operací provedených v jeho prospěch jinou osobou. Dle platné právní úpravy banky v rámci opatření proti legalizaci výnosů z trestné činnosti, nezřizují anonymní účty (Máče, 2006).

Zřizování a vedení běžných účtů věnuje pozornost také Evropská komise, zejména pokud jde o účet spotřebitele. Banky zřizují účty na základě písemné smlouvy, v rámci které banky vyžadují další doklady, které osvědčují právní subjektivitu a dokládají totožnost klienta, takže jde provést jeho řádnou identifikaci. Tyto doklady spolu s podpisovým vzorem k účtu a smlouvou o běžném účtu tvoří nedílnou součást tzv. klientské dokumentace (Schlossberger, 2012).

3.4.2 Elektronické bankovnictví

Mezi platební prostředky elektronického bankovnictví můžeme zařadit **homebanking** (ovládání účtu, včetně plateb z domova), **phonebanking** (ovládání účtu prostřednictvím pevné telefonní linky), **GSM banking** (ovládání účtu prostřednictvím mobilního telefonu) a **internetbanking**. (Černohorský, Teplý, 2011).

Platby mobilním telefonem probíhají bezhotovostně v reálném čase prostřednictvím bezdrátových sítí, kde bezpečností řešení se stává velmi důležitým faktorem (Raina, 2015).

Homebanking - jedná se o způsob komunikace klienta a banky za pomoci osobního počítače vybaveného speciálním softwarem, přičemž samotný přenos dat probíhá prostřednictvím modemu a telefonní linky, ISDN nebo internetu. S rozvojem internetu se řada funkcí homebankingu a internetového bankovnictví prolíná a doplňuje. Již dnes tyto dvě oblasti splývají a jen těžko je můžeme striktně oddělit. Bezpečnost komunikace je zajištěna prostřednictvím digitálního podpisu, šifrováním zpráv použitím šifrovacích algoritmů DES/RSA a certifikací veřejných klíčů (Přádka, Kala, 2000).

Phonebanking - je aplikací založenou na komunikaci klienta s bankou prostřednictvím telefonu tak, že klient komunikuje hlasem s živím pracovníkem banky nebo tlačítky buď s živím operátorem, nebo hlasovým informačním (Interactive Voice Response). Bezpečnost komunikace je založena na identifikaci klienta a ověření jeho totožnosti prostřednictvím použití jedinečného identifikačního čísla (PIN) a bezpečnostního přístupového hesla (Máče, 2006).

GSM Banking - představuje pokročilejší formu bankovnictví, která ke svému fungování vyžaduje GSM telefon, nejlépe s podporou přídavných funkcí SIM karty – tzv. SIM toolkit. Základním prvkem je bankovní aplikace uložená na kartě, která zprostředkovává přes intuitivní rozhraní komunikaci mezi bankou a klientem. Komunikace je šifrovaná, přístup je zabezpečen bankovním PINem. Aplikace může obsahovat i funkce pro generování dalších přístupových kódů. GSM Banking k jednomu účtu lze provozovat pouze z jedné SIM karty (Matyáš, Krhovják a kol., 2008).

Internetbanking – jde o aplikaci, s využitím komunikace přes internet, která nevyžaduje speciální hardware a připojení klienta na aplikaci v bance zajišťuje jednoduchý software instalovaný v osobním počítači klienta. Existují aplikace vázané na konkrétní osobní počítač klienta i aplikace přenosné, které je možné aktivovat z kteréhokoliv počítače po zadání hesla (Polouček a kol.,2006).

3.4.3 Platební karty a bankomaty

Platební karty jsou bezesporu nejstarším a v současnosti také nejpoužívanějším instrumentem, který poskytuje vzdálený přístup k bankovnímu účtu elektronickou cestou. Nejčastěji prostřednictvím platebních terminálů obchodníků, bankomatů nebo internetu (Máče, 2006).

Prostřednictvím platební karty lze provádět dvě základní věci, platit za zboží a služby v obchodě, nebo vybírat hotovost u bankomatu. Vzhledem ke svému názvu by se měla platební karta využívat k placení a ne k výběru z bankomatu. Často je ale klientem využívána jen proto, aby jejím prostřednictví si v den připsání své mzdy u nejbližšího bankomatu vybral celý zůstatek na účtu a nemusel chodit do své banky (Přádka, Kala, 2000).

Vydavatelé platebních karet

Platební karty vydávají prostřednictvím bank tzv. karetní asociace, těmi největšími, dle hlediska počtu držitelů platebních karet, jsou EuroPay/MasterCard, VISA, JCB, American Express a Diners Club. Dle Kalabise, lze podle hlediska vydávání platební karty a zpracování platebních transakcí, dělit jednotlivé účastnické banky v mezinárodní karetní asociaci na banky:

- **vydavatelské**, které se specializují na vydávání platebních karet,
- **zpracovatelské**, které se specializují pouze na zpracování platebních transakcí,
- **vydavatelské i zpracovatelské,** které spolu s vydáváním platebních karet zpracovávají i platební transakce uskutečněné prostřednictvím platebních karet jak u obchodníka, tak i v síti bankomatů (Kalabis, 2012).

Dělení platebních karet

Platební karty můžeme rozlišovat podle různých kritérií, nejčastěji autoři odborné literatury karty dělí dle způsobu zúčtování plateb nebo techniky záznamu dat.

Dle způsobu zúčtování prováděných plateb u obchodníka a výběrů z bankomatu, lze platební karty dělit na čtyři druhy.

- **charge karta**, držitel karty provede úhradu provedených transakcí na základě zaslaného výpisu, kerý je zaslán vydavatelem karty
- **kreditní karta**, jde o kartu, kdy banka s jejím držitelem sjednává úvěrový rámec, do jehož výše lze provádět platby a výběry z bankomatu,
- **debetní karta**, jedná se o kartu, kterou banka vydává klientovi k jeho běžnému účtu, platby lze provádět do výše zůstatku na účtu,
- **elektronická peněženka,** předplacená karta, u které se platební operace ověřují na úrovni čipové karty a platebního terminálu. Kredit se dobíjí u provozovatele systému proti zatížení účtu klienta (Polouček a kol.,2006).

Dle techniky záznamu dat na kartě, můžeme platební karty dělit na čtyři níže uvedené druhy.

- **embosovaná karta**, identifikační údaje jsou na této kartě vyraženy reliéfním písmem z důvodu možného snímání údajů v mechanických snímačích obchodníků (imprinter),
- **karta s magnetickým záznamem,** data, zejména identifikační údaje a provedené transakce, jsou zaznamenána na magnetický proužek, což umožňuje provádění elektronických transakcí platební kartou,
- **čipová karta,** data jsou zaznamenána v mikročipu, který je umístěn na přední straně karty. Výhody spočívají ve vyšším stupni bezpečnosti, širšího využití díky paměti čipu a možnosti lokálního ověření identifikačních údajů (PIN),
- **karta s laserovým záznamem,** data jsou zaznamenána do podkladové vrstvy laserovou technologií. Výhodou je vysoká kapacita záznamu, nevýhodou jednoduché kopírování (Máče, 2006).
- **bezkontaktní karta,** je platební karta, či jiný token (nejběžněji v podobě chytrého telefonu či hodinek), která díky integrované anténce funguje do vzdálenosti asi 5 centimetrů od čtečky platebního terminálu. To umožňuje jejímu vlastníku ponechat kartu při platbě v peněžence (obr. 1).

Obr. 1 Čipové platební prostředky

Zdroj: www.mesec.cz

Karetní systémy

V současné době se můžeme setkat s pěti největšími kartovými asociacemi. Účast platebních institucí v jednotné mezinárodní síti je vždy několikanásobně levnější a účinnější. Mezinárodní platební systémy můžeme rozdělit na bankovní a nebankovní.

Bankovní asociace

- VISA International,
- Europay/MasterCard.

Nebankovní asociace

- American Express,
- Diners Club International,
- JCB (Přádka, Kala, 2000).

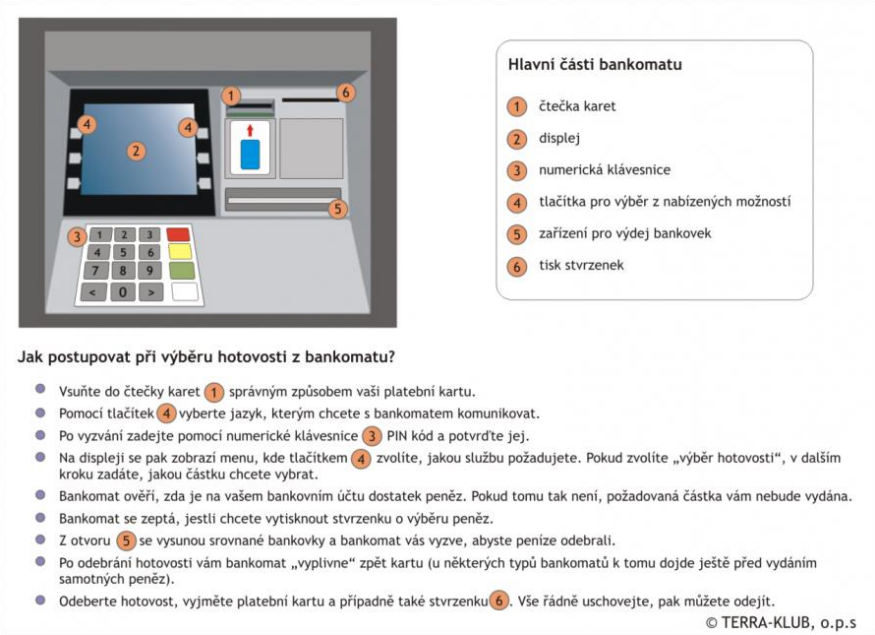
Bankomaty

Platební karty jsou poměrně často využívány k výběru hotovosti z bankomatu. Bankomat (ATM – automatic teller machine) je český název pro zařízení na výdej peněz klientům prostřednictvím jejich platebních karet. Bankomat tvoří několik základních částí.

- **trezor,** obsahuje kazety na bankovky, které jsou plněny v bankách. Kazeta se mění kus za kus a nevydaná hotovost se z kazety vytahuje až na pracovišti v bance.

- **operátorská část,** je tvořena PC s ovládáním pro operátora. Je využívána při servisu a přestavování parametrů bankomatu.
- **provozní část,** ve které jsou vlastní zařízení potřebná pro komunikaci s klientem, a výdej hotovosti (Polouček a kol.,2006).

Obr. 2 Hlavní části bankomatu



Zdroj: TERRA-KLUB

Dnes se téměř výhradně používají on-line bankomaty, které jsou napojeny prostřednictvím datové sítě do autorizačního centra a ověřují prováděnou transakci v reálném čase přímo u vydavatele platební karty. Transakce jsou ověřeny během několika sekund. U tohoto postupu není na magnetickém proužku zaznamenán ani PIN, ani finanční limit karty (Juřík, 2006).

3.5 Zabezpečení bezhotovostních platebních transakcí

Tato kapitola se bude zabývat způsobem zabezpečení bezhotovostních platebních operací, prováděných především prostřednictvím služby internetového bankovnictví nebo pomocí platebních karet.

Prostřednictvím služby internetového bankovnictví klienti bank pracují se svými penězi na běžném účtu, který mají veden u své banky. Bezhotovostní platby jsou prováděny zejména formou trvalého a jednorázového příkazu k platbě, nebo příkazem k inkasu. Při provádění uvedených platebních operací je prvořadou záležitostí zajištění jejich bezpečnosti. Ta je zajištěna systémem ochrany internetového bankovnictví, který se skládá z několika prvků, které jsou vzájemně propojeny.

První ochranou klienta banky proti možnému zneužití jeho bezhotovostních peněžních prostředků na běžném účtu je způsob, jakým se do internetového bankovnictví přihlašuje. Jako základní způsob přihlášení se používá klientské číslo a heslo, který slouží k autentizaci uživatele. Pro autorizaci platebních transakcí, potvrzení platebních příkazů nebo změn v internetovém bankovnictví se používají různé způsoby zabezpečení (www.bezpecnyinternet.cz).

Bezpečnost systému elektronického bankovnictví je postavena jak na zabezpečení aplikace, tak i na zajištění fyzické bezpečnosti. Jedná se především o bezpečnost organizační a technologickou. V rámci organizační bezpečnosti je zejména důležité zajištění dodržování základních bezpečnostních zásad, a to především princip čtyř očí, kdy u důležitých operací je nutné přítomnost dvou oprávněných osob, oddělení rolí operátorů a správců systému, kdy každému zaměstnanci je umožněn přístup pouze k části systému banky (Přádka, Kala, 2000).

3.5.1 Fyzická bezpečnost systému a zabezpečení komunikačních kanálů

Fyzická bezpečnost

Bezpečnost platebních systémů je zajišťována jak prostřednictvím informačních technologií, zajišťujících bezpečnost informací, tak i fyzickým zabezpečením. Tím, jak informační technologie stále více zasahují do reálného života v rámci platebního styku, se fyzická a kybernetická bezpečnost stále více prolínají.

Bezpečnost platebních systémů je zajišťována jak prostřednictvím informačních technologií, zajišťujících bezpečnost informací, tak i fyzickým zabezpečením. Tím, jak informační technologie stále více zasahují do reálného života v rámci platebního styku, se fyzická a kybernetická bezpečnost stále více prolínají.

Fyzická bezpečnost informačních zařízení je zajišťována s pomocí takových technologií, které zabezpečují informaci proti fyzickému útoku. Vzhledem k tomu, že jsou informační a komunikační zařízení instalována v nezabezpečením prostředí, např. platební terminály nebo bankomaty, je jejich fyzická bezpečnost prioritou.

Dle Matyáše, Krhovjáka a kol. mezi metody fyzického zabezpečení komunikačních zařízení patří:

Evidence průniků, je využívána v rámci bezpečnostní politiky systému. Detekce průniku a jeho evidence je zajištěna pomocí chemických a mechanických prostředků (např. barvivo, pečetě, zámky).
Odolnost proti průnikům, je zajišťována pomocí ocelových krytů a chemikáliím odolným materiálů. U čipových platebních karet jsou používány ochranné vrstvy na čipu.
Detekce průniků, která je zajištěna pomocí bezpečnostních elektronických čidel a obvodů, připojených ke krytu, či jiným bezpečnostním prvkům.
Odpověď na průniky, zahrnuje mechanismy aktivované při detekci průniku. Zpravidla jejich aktivací dochází k zničení zařízení nebo vymazání jeho paměti.

Technologické centrum

Stěžejní roly v bezhotovostních platbách mají autorizační a zúčtovací systémy karetních asociací.

Příkladem technologického centra je technické zázemí provozované společností MasterCard, které se nazývá Banknet. V rámci Banknetu je napojeno 25 000 bank, vydávajících platební karty MasterCard a Maestro. Centrum systému leží v blízkosti amerického města St. Louise, záložní centrum se nalézá v Missouri. Spojení s bankami je zajištěno prostřednictvím privátní datové sítě (VPN), provozované společností AT&T (Juřík, 2006).

Kryptografická ochrana

Elektronický platební styk je realizován prostřednictvím datových sítí. Data platebních transakcí jsou zpracovávány převážně komunikačními servery. Dále se na zpracovávání informací podílejí ještě databázové servery, které v rámci zpracovávání požadavku uživatele pracují s databází, ze které získávají požadované údaje, modifikují aktuální data a nové informace do databáze ukládají (Máče, 2006).

Pro zajištění bezpečné komunikace s bankou, která probíhá prostřednictvím datové sítě, jsou použity prvky kryptografické ochrany. Citlivá data jsou šifrována, aby nemohla být čtena neoprávněnou osobou a změněna jejich integrita.

Základem bezpečného a spolehlivého platebního systému je maximální zajištění bezpečnosti datového toku. Jelikož se banky snaží minimalizovat své náklady, tak jsou v současnosti využívané standardizované technologie, které pracují v on-line režimu. Technické řešení systému tak nepředstavuje zásadní problém. Datové toky jsou zabezpečeny prostřednictvím HTTPS tedy SSL certifikátem.

Velmi střeženým tajemstvím banky, v rámci kryptografické ochrany komunikace, je bankovní šifrovací soukromí klíč. Tento klíč je uložený v šifrátoru, počítači uloženém ve speciálním plášti. Šifrátor provádí pouze kryptografické operace, vždy chrání tajemství

v podobě soukromého klíče, a to i při fyzickém útoku na zařízení. Jedinou výjimkou je zálohování klíče. Při zálohování je klíč rozložen na dvě čipové karty. Každou z karet drží pouze jedna pověřená osoba. Třetí osoba zná heslo k soukromému klíči. Ze zálohy je možné soukromí klíč obnovit, a to v případě jeho ztráty (Přádka, Kala, 2000).

Z důvodů zajištění technologické funkčnosti, omezení chyb lidského faktoru či selhání kontrolních mechanismů, vytvářejí banky hlavní a záložní technologická centra a zálohují cenná data o provedených platebních transakcích (Schllossberger, 2012).

Autentizace uživatelů a autorizace transakcí

Pro bezpečnou komunikaci mezi klientem a bankou je stěžejní zajištění tří atributů. **Důvěrnost zpráv**, což znamená, že si předmětné sdělení může přečíst pouze jeho adresát. Toto banky řeší šifrováním komunikace. Dalším atributem bezpečného internetového bankovnictví je **autentizace protistrany**, tedy komunikuji s tím, s kým si myslím. To je řešeno šifrováním a elektronickým klíčem. Tím posledním je **průkaznost původu zprávy**, která je zajištěna prostřednictvím certifikace dat elektronickým klíčem a digitálního podpisu (Přádka, Kala, 2000).

V principu existují tři základní metody autentizace uživatelů, lišící se typem prostředků, které jsou pro autentizaci použity. Metody tedy mohou být založeny buď na něčem, co daný uživatel zná (nějáká tajná informace, např. PIN, heslo či přístupová fráze), na něčem, co daný uživatel má (nějaký předmět/token jako např. platební karta), nebo na něčem, čím daný uživatel je (nějaká biometrická informace jako např. otisk prstu). Z důvodu eliminace výhod a nevýhod jednotlivých metod se často volí jejich vhodná kombinace (Matyáš, Krhovják a kol., 2008).

Autentizační faktory

- **znalost,** kromě výše uvedeného PIN a hesla, sem patří i výběr obrázku podle své preference, nakreslení gesta nebo znaku (např. pro Android). Oblíbené jsou také osobní otázky.

- **vlastnictví,** sem mimo jiné můžeme zařadit hardwarové tokeny (např. RSA SecurID), platební karty, mobilní telefony (aplikace využívající IMEI) a SIM karty.
- **biometrie,** zde si lze představit, že se jedná o prvek, který zahrnuje charakteristiky svého nositele. Rozšířený je otisk prstu, využívaný ve sféře notebooků a další dotykové mobilní techniky. Dalším prvkem může být sken očnice, rozpoznání obličeje nebo hlasu.

V současné době je diskutován i faktor **geolokace**, který může být využíván v boji proti útokům na MFA. Jedná se o využití informací o tom, kde a kde se majitel nachází (www.computerworld.cz).

V rámci jednodušších metod autentizace se v rámci internetového bankovnictví používá jméno, popř. klientské číslo a heslo. Jako další bezpečnostní prvek je možnost zaslání sms na mobilní telefon klienta při každém přihlášení do internetového bankovnictví. Prostřednictvím SMS je možné zasílat zprávy o aktuálních pohybech peněžních prostředků a zůstatků na účtu klienta. Uživatel účtu má tak neustále přehled o pohybech peněz na svém účtu, což snižuje pravděpodobnost případu podvodného jednání.

Příkladem složitějšího způsobu autentizace je použití elektronického podpisu, což je asymetrický šifrovací algoritmus. Ten je používán při komunikaci prostřednictvím speciálních programů. Program je postaven na bázi tajného a veřejného klíče. Veřejný klíč musí být certifikován certifikační autoritou. Odesílatel data zašifruje prostřednictvím svého tajného klíče a veřejného klíče adresáta. Adresát data s pomocí svého tajného klíče a veřejného klíče odesílatele dat rozšifruje, a provede autentizaci odesílatele (Máče, 2006).

Při komunikaci mezi klientem a bankou, v rámci internetového bankovnictví, jsou autentizační data přenášena nezabezpečeným prostředím a mohou být zachycena a zneužita. Šifrování, či hašování autentizačních dat není samo o sobě dokonalé řešení. Z tohoto důvodu jsou bankami používány složitější autentizační schémata, tzv. **autentizační protokoly.** Uvedené protokoly fungují na principu výzva-odpověď, kdy se ověřuje správnost a čerstvost autentizačního požadavku, sdílené tajemství, které je zabezpečeno s využitím prvků kryptografické ochrany (Matyáš, Krhovják a kol., 2007).

Autentizační metody

Hesla

Heslem je alfanumerický řetězec znaků, jedná se o jednoduchý a rozšířený prostředek pro autentizaci uživatelů. Uživatel zadá uvedený řetězec, který systém porovná se svou databází. Bezpečnostním rizikem tohoto způsobu autentizace je nebezpečí odpozorování, nebo prolomení hesla pomocí nástrojů generujících hesel, např. slovníkový útok. Zvláště nebezpečné je používání stejných hesel, pro více aplikací. Banky jsou tímto nuceny zvyšovat nároky na kvalitu řetězce, který tvoří heslo. Dalším bezpečnostním prvkem je perioda změny hesla. Zmiňovaná bezpečnostní opatření snižují komfort pro uživatele bankovnictví (www.arrowecs.cz).

Dvoufaktorová autentizace

Dvoufaktorová autentizace může být používána na zařízeních, která umožňují ukládání a zadávání potřebných údajů. Aplikace funguje na bázi co uživatel má (smartphone) a co zná (např. jednorázové heslo). Autentizace probíhá s využitím šifrovacích technik. Uživatel má k dispozici šifrovací klíč a jednorázové heslo. V minulosti se používaly hardwarové tokeny, které generovaly jednorázová hesla. Během posledních let se stále častěji používají sms zprávy a další mobilní technologie (Šnajdr, 2013).

Jako jedna z nejjednodušších a tak autentizačních metod je používána autentizace prostřednictvím **jména** a **hesla** s možností odesílání **sms** zprávy na mobilní telefon klienta banky při každém přihlášení. Krátká textová zpráva obsahuje kromě potvrzovacího kódu i telefonní číslo pro zablokování (Máče, 2006).

Třífaktorová autentizace

Podle hlediska bezpečnosti autentizace je nejvyšším používaným způsobem třífaktorová autentizace, která používá jednu z metod z každé, výše uvedených skupin autentizačních faktorů. Systém je uspořádán tak, že biometrická informace (např. otisk prstu) je zpracovávána a nasnímána tokenem (např. smartphone), PIN nebo heslo je zadáno do zařízení, které je pod kontrolou uživatele a autentizačního serveru. K úspěšnému provedení autentizace je potřebná spolupráce tokenu, v rámci kterého je ověřována biometrická informace (Matyáš, Krhovják a kol., 2007).

Společnost MasterCard letos představila studii o vlivu inovací, jejímž zjištěním bylo, že občané České republiky rychle přijímají nové technologie. Dalším zjištěním studie bylo, že 35% českých respondentů preferuje jako nejpohodlnější způsob své autentizace otisk prstu, kdy takoví způsob používá 3% populace. Celkem 50% populace autentizaci prostřednictvím otisku prstu považuje za bezpečnou. Z výše uvedeného vyplývá, že čtečky otisků prstů v mobilních telefonech a dalších mobilních zařízení mají potenciál dalšího rozvoje (www.nearfield.cz).

3.5.2 **Bezpečnost internetového bankovnictví**

Dle Přádky a Kaly lze dělit internetové bankovnictví na dva druhy. Podle kritéria úrovně komfortu pak dělíme internetové bankovnictví na neplnohodnotné, které je vázáno na použití konkrétního počítače s nainstalovaným bezpečnostním softwarem (využívajícím digitální certifikáty a podpisy), a na plnohodnotné, kde bankovnictví je přístupné z libovolného počítače s připojením na internet.

Při využití neplnohodnotného internetového bankovnictví se používá nejčastěji speciální bezpečnostní software, který pro komunikaci s bankou pracuje s digitálním podpisem, což je digitální asymetrický šifrovací algoritmus. Tento software je postaven na bázi dvou klíčů, tajného a veřejného. Veřejný klíč je certifikován veřejnou certifikační autoritou. Banka i klient mají dva klíče. Zabezpečení komunikace probíhá tak, že odesílatel data zašifruje pomocí svého tajného a veřejného klíče protistrany. Ta pomocí svého tajného klíče a veřejného klíče odesílatele data rozšifruje (Máče, 2006).

V rámci plnohodnotného internetového bankovnictví, pro zajištění bezpečnosti komunikace mezi bankou a klientem, se vyžaduje, aby měly banka a klient přístupné zařízení umožňující vzájemnou autentizaci obou stran komunikace. Toto zařízení není přímo spojeno s konkrétním počítačem, obě strany komunikace prostřednictvím vzdáleného přístupu si mezi sebou vyměňují vygenerované kódy. V počítači klienta není nainstalován žádný speciální software, internetové bankovnictví své banky může využívat z jakéhokoliv počítače (Přádka, Kala, 2000).

Předpokladem bezpečného přímého bankovnictví je zabezpečený přenos informací mezi bankou a klientem v obou směrech. K přenosu informací dochází prostřednictvím veřejné datové sítě „INTERNET“ na kterou je počítač klienta připojen.

Bezpečnostní prvky internetového bankovnictví

Způsob přihlášení

Velmi důležitým prvkem zabezpečení internetového zabezpečení je způsob, jakým se do něho přihlašujeme. Nejběžněji se pro přihlášení používá klientské číslo a heslo. Doplňkovým prvkem bývá často přihlašovací sms zpráva, kdy klient po zadání klientského čísla a hesla obdrží časově omezený jednorázový kód. Výhodou je, že přihlašování do internetového bankovnictví je bezpečnější i z počítačů, které používá více uživatelů, např. v kavárně nebo ve škole. V případě, že dojde opakovaně ke špatnému zadání přihlašovacích údajů, zpravidla třikrát, dojde k automatickému zablokování služby bankovnictví.

Některé banky, jako prvek ochrany před sledovacím spywarem, nabízejí možnost zadávání přihlašovacích údajů na tzv. elektronické klávesnici. Ta se zobrazuje na obrazovce počítače a jednotlivé znaky klient vybírá myší.

Klientské číslo a heslo pro první přihlášení je nejběžněji klientovi zasláno prostřednictvím poštovní přepravy do vlastních rukou. Velmi důležitá je kontrola neporušení zásilky klientem. V případě porušení zásilky, klient zásilku nepřevezme a s popisem situace zašle zásilku zpět, a požádá o zaslání nového klientského čísla a hesla.

Autorizace transakcí

V rámci služby internetového bankovnictví lze realizovat řadu finančních operací, nejčastěji se jedná o jednorázový příkaz, zadání trvalého příkazu k platbě nebo souhlasu s inkasem. Aby tyto operace byly bezpečné, tak je vyžadována jejich autorizace. V rámci přihlášení v internetovém bankovnictví, je autorizace nejběžněji prováděna pomocí autorizační sms zprávy. Tu klient obdrží na svůj mobilní telefon po vyplnění příkazového formuláře v aplikaci bankovnictví a kliknutí na odkaz pro zaslání autorizační sms. Další způsob autorizace je prostřednictvím klientského certifikátu, který je uložen na čipové

kartě. Jedná se o tajný klíč klienta, kterým je příkaz klienta bance podepsán. Bez držení tokenu, kterým je např. zmiňovaná čipová karta, nelze tajný klíč získat. Banka transakci provede, po ověření zprávy dle podpisu s přiděleným certifikátem, který klient obdržel od banky.

Komunikační zařízení

Služby internetového bankovnictví v České republice používají čtyři pětiny lidí. Pomocí chytrého telefonu pak komunikuje s bankou každý čtvrtý klient. Důležitým prvkem ochrany proti zneužití internetového bankovnictví je bezpečný a dobře chráněný počítač nebo chytrý telefon. Základem je aktualizovaný a legální operační systém počítače a antivirový program. Dalším důležitým prvkem je antispyware, což je protišpionážní program, který kontroluje data, která přicházejí do počítače. Vyhledává škodlivý software, který ohrožuje počítač uživatele a zamezuje jeho přístupu do počítače (www.aktualne.cz).

3.5.3 Bezpečnost platebních karet a bankomatů

Bezpečnostní prvky platební karty

Magnetický proužek

Magnetický proužek karty obsahuje 2 nebo tři záznamové stopy, na kterých jsou zaznamenána data karty. Na první stopě jsou zaznamenány údaje o číslu karty a jménu jejího držitele pomocí až 79 alfanumerických znaků. Druhá stopa obsahuje opět číslo karty zaznamenané pomocí až 40 alfanumerických znaků. Je určena pro použití karty v on-line režimu. Třetí stopa může zaznamenat až 107 alfanumerických znaků, tato data mohou být přepisována. Je určena pro použití v of-line režimu a umožňuje ověření PIN kódu a zaznamenání zůstatku. Celková záznamová kapacita proužku je 1288 bitů (Dvořák, 2005).

Z výše uvedeného je patrná jedna z nevýhod magnetického záznamu dat, kterou je malá kapacita záznamu. Oproti čipové kartě se dají zaznamenaná data na magnetickém proužku karty snáze zkopírovat. Ochrana PIN kódu na magnetickém záznamu je oproti čipu na nižší úrovni.

Čipová technologie

V současnosti je čipová technologie povinná pro všechny země evropského hospodářského prostoru, které vydávají platební karty pod hlavičkou VISA nebo Europay/MasterCard. Struktura a umístění čipu podléhají mezinárodní standardizaci obecně označované jako EMV (Europay/MasterCard, VISA). Vzhledem k tomu, že je výměna karet zdlouhavá, přikročily banky k emisi karet hybridních, tzn. karet, které jsou opatřeny jak čipem, tak magnetickým proužkem (Schlossberger, 2012).

Rozhodující pro zavedení čipových platebních karet bankami bylo, že umožňují použití karet při platbě menší částky, díky bezkontaktní čipové technologii (Juřík, 2012).

Čipové karty lze dělit na tři druhy, na paměťové karty, u nichž jsou data pevně uložena a nelze je měnit (například telefonní karty), na logické karty, u těchto karet se vlastník může identifikovat a inteligentní karty, u kterých je umožněno po autentizaci oprávněného držitele karty měnit vložená data či karty programovat (Jílek, 2013).

Platba kartou u obchodníka

Při platbě čipovou platební kartou v kamenném obchodě, se karta vkládá do platebního terminálu, kde musí být po celou dobu transakce vložena. Zákazník se řídí pokyny na displeji terminálu. K ověření je vyžadováno zadání PINu na klávesnici terminálu pro ověření držitele karty. V případě platby bezkontaktní kartou, držitel přiloží kartu k bezkontaktnímu terminálu, do určité částky, uvedené v obchodních podmínkách banky, není vyžadováno zadání PINu. Při překročení této částky, je držitel bezkontaktní karty vyzván k zadání PINu.

Autorizace platby kartou

Podpis držitele – tento způsob autorizace je s nástupem čipových karet na ústupu, v současné době se jedná o ojedinělý způsob autorizace platby kartou.
Autorizace PINem – v současnosti jde o převládající způsob autorizace. Je velkým posunem, ať už z pohledu komfortu při placení kartou, tak i úrovní bezpečnosti.

Platební terminál

Moderní platební terminály umožňují platby kartou s magnetickým proužkem, čipem i bezkontaktní technologií. Můžeme se při platbě u obchodníka setkat s terminály, které umožňují elektronický záznam podpisu držitele platební karty a jeho zaslání zúčtovací bance obchodníka k uložení do příslušné databáze (Juřík, 2006).

POS terminál (Point of sale)

Platební terminály umožňují platby prostřednictvím výše uvedených typů platebních karet. Za tímto účelem jsou vybaveny čipovou čtečkou karet, čtečkou magnetického proužku a bezkontaktní čtečkou. Bezkontaktně je možné platit jak bezkontaktní kartou, tak mobilním telefonem nebo jiným zařízením s bezkontaktní platební metodou (www.unicreditbank.cz).

Obr. 3 Platební terminál

Zdroj: www.terminalzdarma.cz

Připojení POS

- **internet, prostřednictvím IP**
- **pevná linka, DIALUP**
- **GSM síť, přenos dat prostřednictví GPRS**
- **wi-fi/bluetooth**

mPOS terminál

Mobilní platební terminál, který využívá bluetooth připojení k smart telefonu nebo tabletu, s připojením k internetu. Můžeme se s ním setkat v malých obchodech nebo při platbě za jízdu TAXI (www.terminalzdarma.cz).

Obr. 4 mPOS terminál

Zdroj: www.terminalzdarma.cz

Experiment zabývající se autorizací platby kartou na terminálu

Za zmínku stojí uvést experiment, která byl proveden v letech 2005 a 2006 na Fakultě informatiky Masarykovi univerzity, zaměřený na bezpečnost plateb kartami v kamenných obchodech. V rámci experimentu bylo mimo jiné zkoumáno, jak je obtížné odpozorovat PIN, pří jeho zadávání na platebním terminálu obchodníka. Výsledkem bylo zjištění, že u platebních terminálů bez ochranného krytu PINpadu bylo úspěšně odpozorováno pozorovatelem 80 % PINů a u platebních terminálů opatřených ochranným krytem PINpadu bylo úspěšně odpozorováno 35,5 % PINů.

Platba kartou na internetu

Nejdůležitějším bezpečnostním prvkem platební karty, při platbě u obchodníka na internetu, je její verifikace. Ta probíhá prostřednictvím platební brány, v podobě 3D Secure, v rámci kterého je ověřována na třech různých místech, na serverech banky, tedy mimo web obchodníka. Obchodník se tak k údajům platební karty nedostane. Dalším prvkem je prověření internetového obchodníka, ke kterému dochází ze strany banky při zpracování smlouvy. Prověřuje se zejména jeho důvěryhodnost, a zda je schopen zajistit dodržování bezpečnostních standardů (www. bankovnipoplatky.com)

3D Secure je mezinárodní standard vyvinutý společnostmi Europay/MasterCard a VISA, podporují jej jak domácí internetoví obchodníci, tak samozřejmě i zahraniční internetové obchody. Platba kartou na internetovém obchodu probíhá tak, že se zvolí platba kartou, zadají se údaje platební karty, následně klient obdrží na mobilní telefon nebo e-mail bezpečnostní kód ze zpracovatelské banky, do otevřeného dialogového okna přepíše obdržený kód, potvrdí platbu a tímto je transakce dokončena (www.erasvet.cz).

V internetovém bankovnictví si klient ke své platební kartě nastaví telefonní číslo, na které budou doručovány autorizační SMS zprávy. V internetových obchodech, které podporují 3D Secure, bude vyžadováno potvrzení autorizačním kódem. Proces je podobný, jako u potvrzení platby v internetovém bankovnictví (www.moneymag.cz).

Zabezpečení bankomatů

V současné době se používají bankomaty, které jsou v on-line režimu. Prostřednictvím datové sítě jsou propojeny s autorizačním centrem banky a prováděnou peněžní operaci autorizují v reálném čase, během několika sekund. V rámci tohoto postupu se na magnetickém proužku platební karty nezaznamenává PIN ani limit karty (Juřík, 2006).

Bezpečnostní prvky bankomatu

Monitoring - zařízení bankomatu je pod neustálým dohledem pracovníků banky. V rámci nastavené bezpečnostní politiky banky jsou stanovená pravidla pro sledování a řešení podvodních jednání, která se neustále vylepšují.

Antiskimmovací nástavec – má často podobu zeleného plastu, který je umístěný na vstupu pro platební kartu. Jeho funkcí je zabránění instalaci skimmovacího zařízení, kterým se kopírují data z platební karty.

Softwarová ochrana - ta má podobu např. programu, který přerušuje pohyb karty při zasunutí do otvoru pro platební kartu, což zamezuje podvodnému načtení dat z magnetického proužku karty.

Kamerový systém – slouží k odhalování a zamezování útokům na bankomaty. Kamery jsou schopny spustit alarm v případě jejich zakrytí nebo vyřazení z provozu a tím upozornit na probíhající zločin.

Ochrana proti průniku – zařízení bankomatu je opatřeno čidly a elektronickými obvody, které detekují fyzické napadení. V případě detekce násilného průniku dojde k znehodnocení uložených bankovek speciální barvou a výmazu uložených dat v paměti zařízení (www.bankovnipoplatky.com).

Obr. 5 Antiskimmovací nástavce

Zdroj: www.policie.cz

Autorizace pomocí PINu

Před provedením požadované finanční transakce se uživatel autentizuje zadáním PINu na klávesnici bankomatu. Ten je okamžitě zašifrován do zašifrovaného PIN bloku, pomocí sdíleného klíče mezi bankomatem a poskytující bankou, která provozuje uvedený bankomat a které je zašifrovaný PIN blok zaslán k on-line autentizaci. Nyní poskytující banka pošle zašifrovaný PIN blok na přepínač, se kterým sdílí jiný, zónový klíč. Musí tedy PIN pomocí prvního klíče dešifrovat a pomocí zónového klíče, který sdílí s přepínačem, zašifrovat. Tento proces se opakuje tak dlouho, dokud zašifrovaný PIN blok nepřekoná všechny přepínače k vydavatelské bance, kde má klient vedený svůj účet (Matyáš, Krhovják a kol., 2008).

4 Vlastní práce

V teoretické části byly představeny vybrané platební instrumenty bezhotovostního platebního styku, které jsou v praxi klienty nejčastěji pří bezhotovostní způsobu platby využívány, a to elektronické bankovnictví a platební karty. Byl vymezen způsob ochrany, která je spjatá s jejich používáním a popsány jednotlivé ochranné prvky, které předcházejí, nebo minimalizují následky podvodných jednání. V úvodu praktické části bude provedeno dotazníkové šetření, v rámci kterého bude zkoumán současný vývoj v oblasti vybraných bezhotovostních platebních instrumentů a praktické zkušenosti uživatelů uvedeních platebních instrumentů a dodržování základních bezpečnostních zásad klienty při platbě u obchodníka nebo při finančních operacích u bankomatu.

Dotazníkové šetření proběhlo v období od 27.10.2016 do 21.11.2016. Dotazníkový formulář byl vyhotoven jak v analogové, tak i v elektronické podobě. V rámci šetření byly získány odpovědi od 76 respondentů. Analogový dotazník byl distribuován v katastru okresů Ústí nad Labem, Děčín a Teplice. Digitální dotazník byl distribuován zejména prostřednictvím internetu.

V dotazníku byly použity uzavřené otázky s možnostmi odpovědí, ano-ne, označením frekvence četnosti, zařazením do škály nebo uvedením jiné možnosti. Předmětem šetření jsou tři tematické okruhy. První tematický okruh je zaměřen na používání elektronického bankovnictví, druhý tematický okruh je zaměřen na používání platebních karet a třetí tematický okruh je zaměřen na chování a dodržování základních bezpečnostních zásad držiteli bezhotovostních platebních instrumentů.

4.1 Dotazníkové šetření

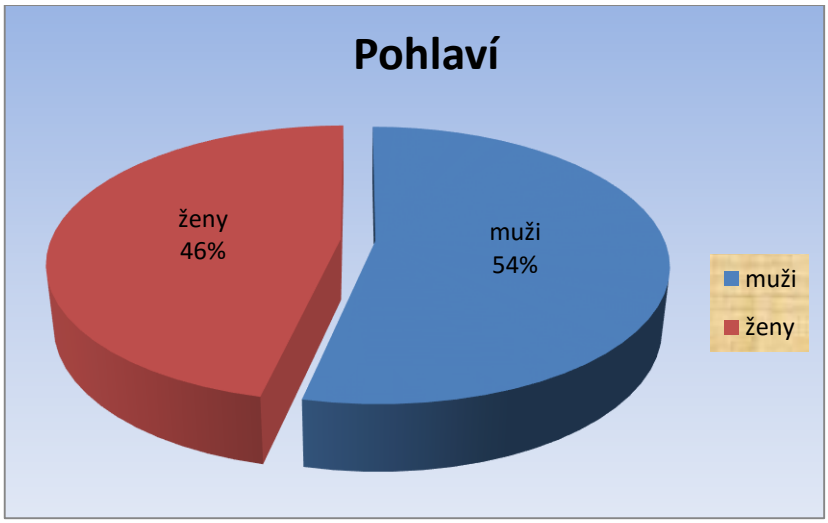
4.1.1 Statistický soubor

Rozsah statistického souboru je tvořen 71 statistickými jednotkami, (dále jen „ respondent“). Z důvodu možnosti posouzení vzájemné závislosti hodnoty statistického znaku respondentů a využívání jednotlivých platebních instrumentů, či dodržování bezpečnostních zásad, byly u respondentů zkoumány tyto statistické znaky, pohlaví, věk a nejvyšší dosažené vzdělání. Cílem dotazníkového šetření je zjištění, zda hodnoty daného znaku mají vliv na bezpečnost používání jednotlivých bezhotovostních platebních instrumentů a zda respondenti jako celek dodržují základní bezpečnostní zásady či doporučení poskytovatelů platebních služeb. Výběr respondentů do statistického souboru byl proveden prostým náhodným výběrem.

Pohlaví

Základní soubor dle zkoumaného statistického znaku respondentů, **pohlaví**, je nepatrně více zastoupeno muži. Ze 76 respondentů uvedlo jako mužské pohlaví 41 dotazovaných a ženské pohlaví uvedlo 35 respondentů. Což můžeme spatřit v níže uvedené vizualizaci pomocí grafu.

Graf 1 Pohlaví respondentů



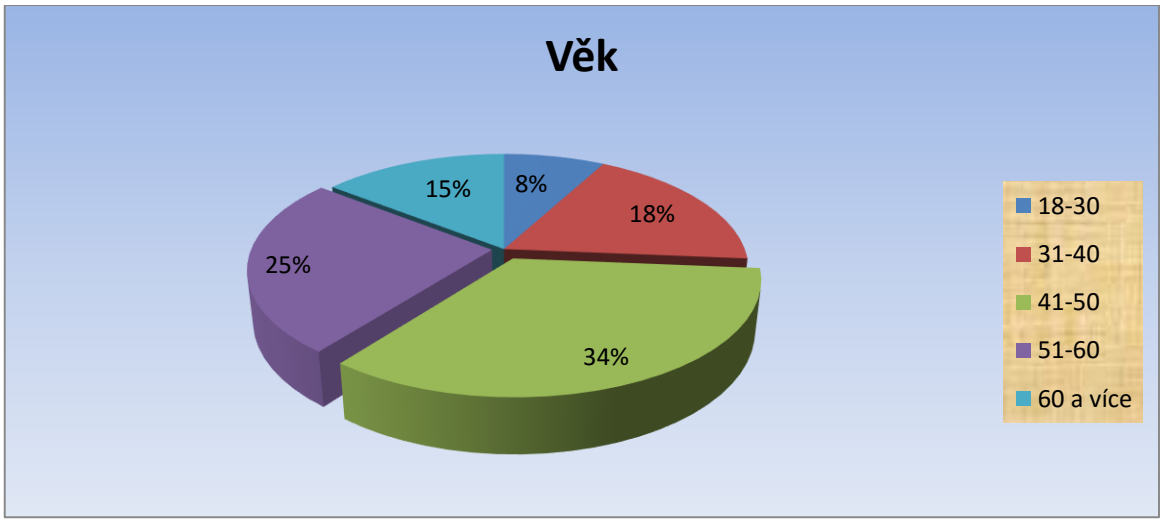
Zdroj: Vlastní zpracování

Věk

Pro účel statistického zkoumání znaku věku, byli respondenti rozděleni do pěti věkových kategorií: 18-30, 31-40, 41-50, 51-60, 60 a více let. Ze 76 respondentů uvedlo 6 respondentů jako věkovou kategorii 18-30 let, dalších 14 respondentů uvedlo kategorii 31-40 let, celkem 26 respondentů uvedlo kategorii 41-50 let, pak 19 respondentů uvedlo věkovou kategorii 51-60 let a 11 respondentů se podřadilo do věkové kategorie 60 a více let.

Jak můžeme vidět v níže uvedené vizualizaci v podobě výsečového grafu, je nejvíce zastoupena věková skupina 41 až 50 let, která je následovaná věkovou kategorií 51 až 60 let. Dohromady tyto dvě uvedené věkové kategorie představují 59% podíl zkoumaného vzorku. Tímto se dotazníkové šetření stává více zaměřené na spíše starší, co se týká životních zkušeností s používáním vybraných platebních instrumentů, zkušenější část populace. Uvidíme, zda se tento předpoklad v dalším zpracování dotazníkového šetření potvrdí nebo zda ho nashromážděná data vyvrátí. Z uvedeného vyplývá předpoklad, že parametry zkoumaného statistického znaku věku budou mít vliv na chování uživatelů internetového bankovnictví a držitelů platebních karet, na dodržování bezpečnostních pravidel při jejich používání při bezhotovostních platbách a úroveň znalostí vybraných ohrožení jejich internetového bankovnictví a platebních karet.

Graf 2 Věk respondentů



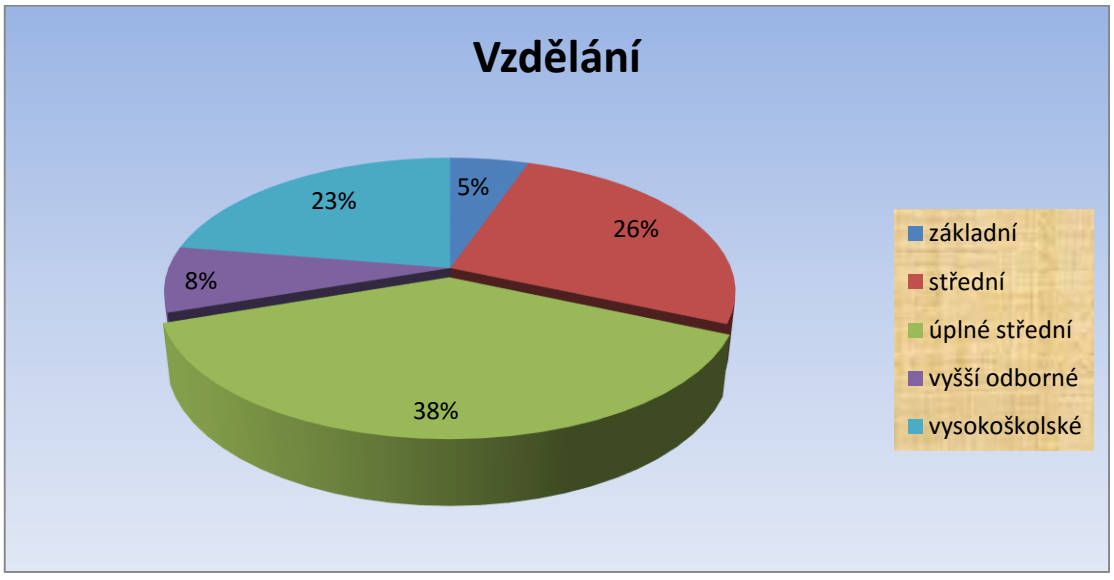
Zdroj: Vlastní zpracování

Vzdělání

Pro účel statistického zkoumání znaku nejvyššího dosaženého vzdělání, byli respondenti rozděleni do pěti stupňů nejvyššího dosaženého vzdělání: základní, střední, úplné střední s maturitou, vyšší odborné a vysokoškolské. Jako nejvýše dosažené vzdělání základní uvedli 4 respondenti, pak za střední stupeň dosaženého vzdělání uvedlo 20 respondentů, celkem 29 respondentů uvedlo stupeň svého vzdělání úplné střední s maturitou, dále 6 respondentů uvedlo vyšší odborné vzdělání a celkem 17 dotazovaných v dotazníku uvedlo vysokoškolské vzdělání.

Jak můžeme vidět v níže uvedené vizualizaci v podobě výsečového grafu, je nejvíce zastoupené vzdělání úplné střední s maturitou. Z uvedeného vyplývá, že celkem 69 % respondentů uvedlo jako nejvýše dosažené vzdělání úplné střední s maturitou a vyšší stupeň vzdělání. Vedle věkové struktury, kterou jsme uvedly výše, dosahuje úroveň vzdělání respondentů dotazníkového šetření převážně vyšších stupňů dosaženého vzdělání. V rámci statistického zpracování dotazníkového šetření bude jedním z cílů i potvrzení předpokladu, zda hodnota statistického znaku, respektive stupeň vzdělání, má vliv na chování respondentů při používání internetového bankovnictví a platebních karet, z pohledu dodržování základních bezpečnostních standardů.

Graf 3 Nejvyšší dosažené vzdělání respondentů



Zdroj: Vlastní zpracování

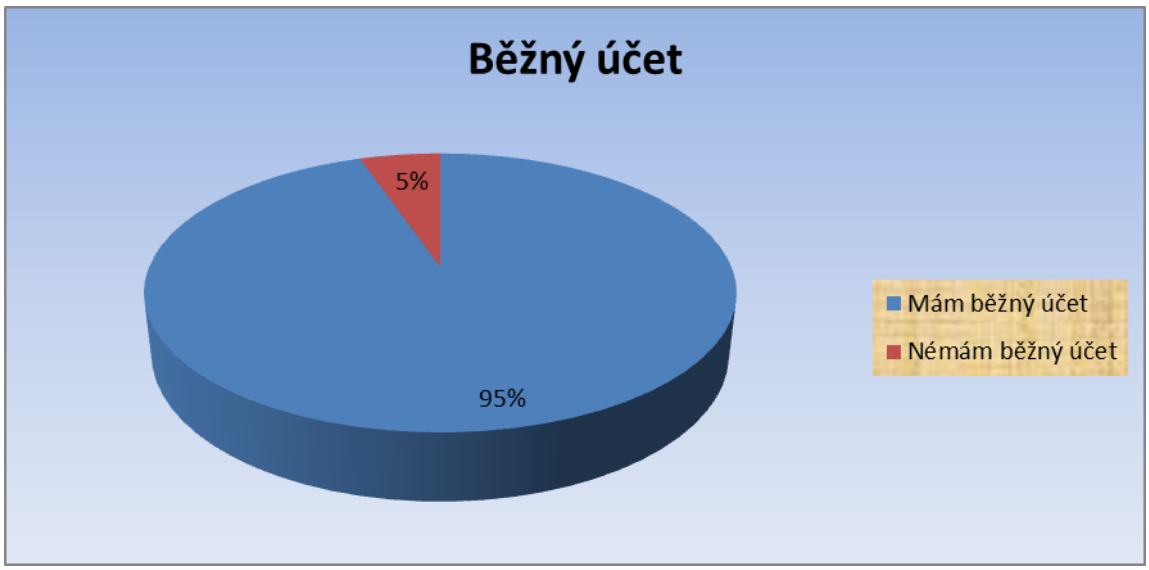
4.1.2 Platební instrumenty

V této podkapitole budou detailněji probrány jednotlivé bezhotovostní platební instrumenty z pohledu jejich používání, dodržování bezpečnostních pravidel a znalostí o možných rizicích při jejich používání. Které bezhotovostní platební instrumenty respondenti využívají, jejich četnost a frekvenci použití, dostupnost a využití bezpečnostních prvků internetového bankovnictví a platebních karet nebo bankomatů. Dále bude předmětem zkoumání komunikační zařízení, prostřednictvím kterého se respondenti přihlašují do svého internetového bankovnictví a způsob zabezpečení uvedených komunikačních zařízení.

Běžný účet

Jako základní prvek bezhotovostního platebního styku je uveden běžný účet, který má zřízen naprostá většina respondentů, jak je patrné z níže uvedené vizualizace, opět v podobě výsečového grafu. Ze 76 respondentů uvedli pouze čtyři respondenti, že nemají zřízen běžný účet. Důvodem je dle jejich sdělení, že používají běžný účet partnera, respektive ve všech uvedených případech partnerky z důvodů úspory nákladů a lepšího přehledu finanční situace domácnosti. K uvedenému lze dodat, že některé banky dnes nabízejí zřízení a vedení běžného účtu zdarma.

Graf 4 Běžný účet



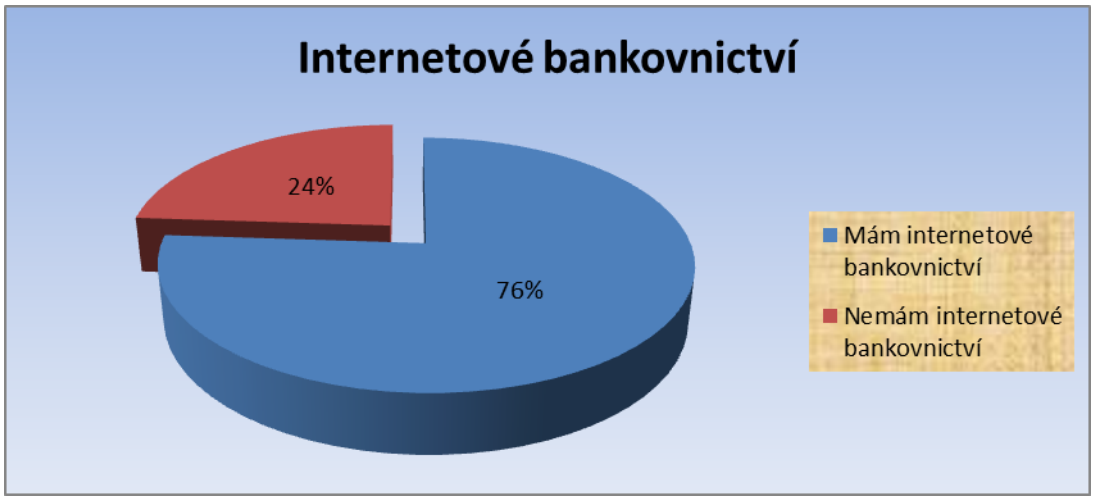
Zdroj: Vlastní zpracování

Internetové bankovnictví

Ke svému běžnému účtu mají zřízeny služby internetového bankovnictví přibližně tři čtvrtiny dotazovaných, v procentním vyjádření to představuje 76 % a pouze 24 % respondentů služeb internetového bankovnictví nevyužívá, jak můžeme vidět v níže uvedené vizualizaci v podobě výsečového grafu. Z uvedeného vyplývá vysoká důvěra respondentů v tento bezhotovostní platební instrument, který v současné době poskytují banky k běžnému účtu zpravidla zdarma.

Internetové bankovnictví přináší klientům vyšší komfort správy svých financí, odpadá nutnost docházky do kamenných poboček bank za účelem vyřízení běžných peněžních operací na běžném účtu, např. příkazů k úhradě, trvalých příkazů nebo inkasa a své finance mají k dispozici 24 hodin denně, sedm dní v týdnu. To jsou důvody, proč je internetové bankovnictví tak hojně využíváno. Z uvedeného grafu je patrné, že důvěra klientů bank v internetové bankovnictví je vysoká. V průběhu šetření si ověříme, zda tato důvěra stojí na rozumných základech, což můžeme posoudit s využitím empirických dat a počtu zjištěných případů podvodného jednání.

Graf 5 Internetové bankovnictví

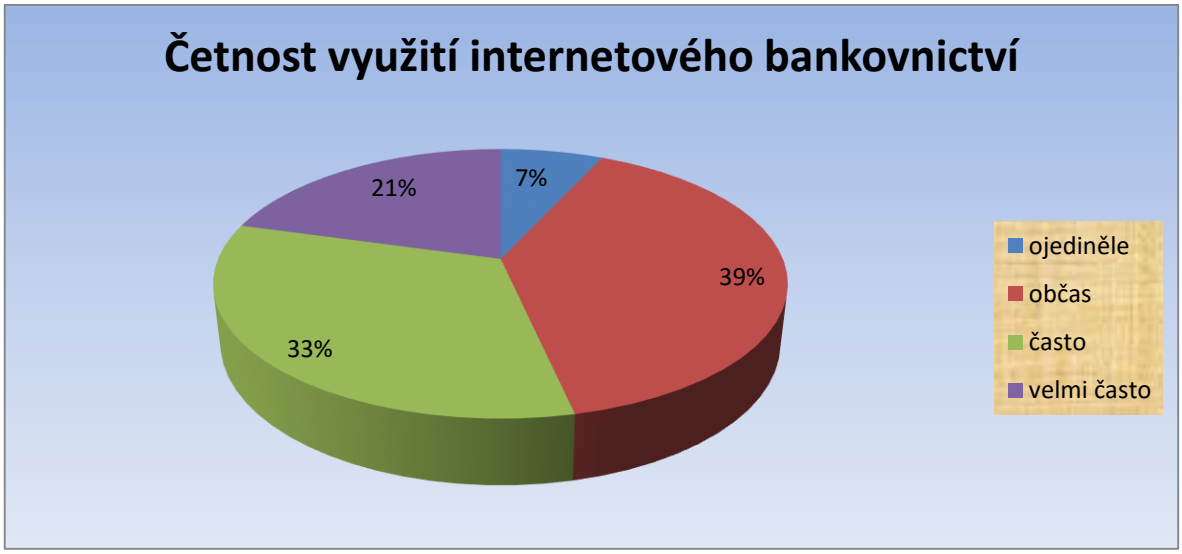


Zdroj: Vlastní zpracování

Četnost využívání internetového bankovnictví

Do svého internetového bankovnictví se většina dotazovaných přihlašuje často, nebo velmi často, jak vyplývá z výsledků dotazníkového šetření, jedná se o 54 % respondentů. Kdy ze 76 respondentů uvedlo, že se přihlašuje do internetového bankovnictví, 4 ojediněle, 23 občas, 19 dotázaných uvedlo často a 12 dotazovaných uvedlo velmi často. Důvody této vyšší frekvence přihlášení mohou být, že respondenti chtějí mít přehled o pohybech peněžních prostředků na svém účtu a aktivně využívají služby internetového bankovnictví. Před návštěvou kamenné pobočky banky, sále častěji vyřizují běžné peněžní operace z pohodlí svého domova, jednak z důvodu lepšího komfortu, tak i z důvodů úspory času a nákladů.

Graf 6 Četnost používání internetového bankovnictví

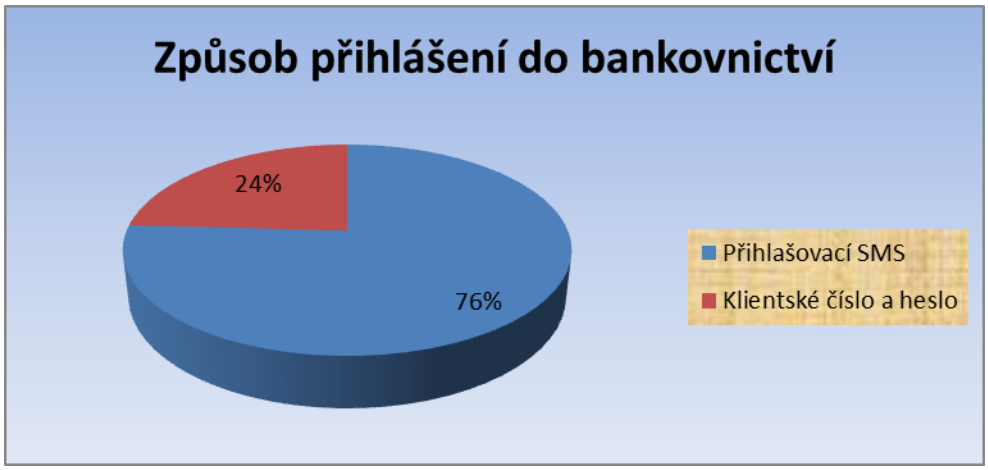


Zdroj: Vlastní zpracování

Způsob přihlášení do bankovnictví

Z níže uvedeného vizuálního zpracování dat v podobě grafu č.7 je patrné, že většina respondentů se do svého internetového bankovnictví přihlašuje prostřednictvím přihlašovacích SMS zpráv, jde o 44 dotazovaných a pouze 14 respondentů se přihlašuje pouze prostřednictvím klientského čísla a hesla. Uvedené vypovídá o vyšším stupni zabezpečení přihlášení do internetového bankovnictví u dotazovaných.

Graf 7 Způsob přihlášení do bankovnictví

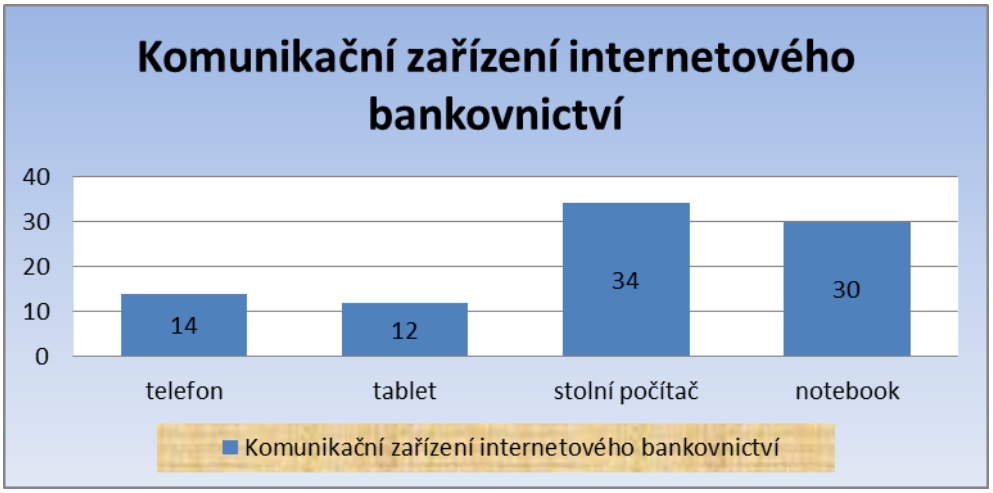


Zdroj: Vlastní zpracování

Komunikační zařízení

Jako prostředek dálkového přihlášení do internetového bankovnictví je nejvíce používán stolní počítač, který jako komunikační zařízení pro přístup k bankovnictví uvedlo celkem 34 dotazovaných, tedy 38 % respondentů, jak je vidět v grafu č. 8. Následuje přihlášení s využitím notebooku, který uvedlo 30 dotazovaných, tedy 33 %. Pouze 14 dotazovaných se přihlašuje i prostřednictvím svého telefonu a 12 respondentů pomocí tabletu. Z uvedeného vyplývá, že většina respondentů se do internetového bankovnictví přihlašuje z bezpečí svého domova.

Graf 8 Komunikační zařízení pro přístup k bankovnictví

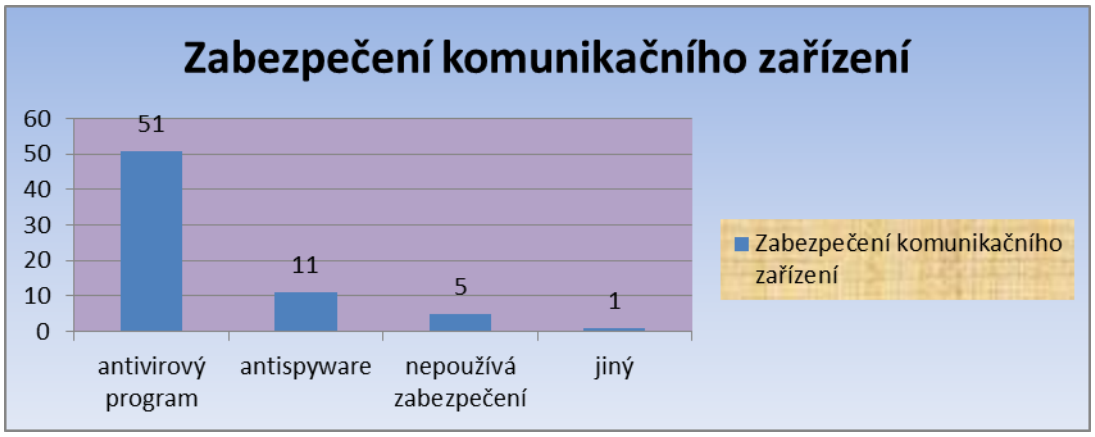


Zdroj: Vlastní zpracování

Zabezpečení komunikačního zařízení

Jedním z důležitých bezpečnostních prvků ochrany internetového bankovnictví je softwarová ochrana klientova komunikačního zařízení, neboť se jedná o nejslabší článek ochrany. Z celkem 58 respondentů, kteří uvedli, že mají zřízeny služby internetového bankovnictví, má 51 dotazovaných ve svém komunikačním zařízení nainstalovaný antivirový program, 11 respondentů používá protišpionážní program a jeden uživatel používá aplikaci Trusteer Rapport, nástroj proti podvrženým stránkám a malware. Pouze 5 respondentů v dotazníku uvedlo, že nepoužívá žádní nástroj ochrany svého zařízení. Naprostá většina uživatelů internetového bankovnictví používá softwarové zabezpečení svého zařízení, čímž i vlastním přičiněním přispívá k vyšší úrovni zabezpečení, uvedené je vizuálně patrné v grafu č. 9.

Graf 9 Ochrana komunikačního zařízení



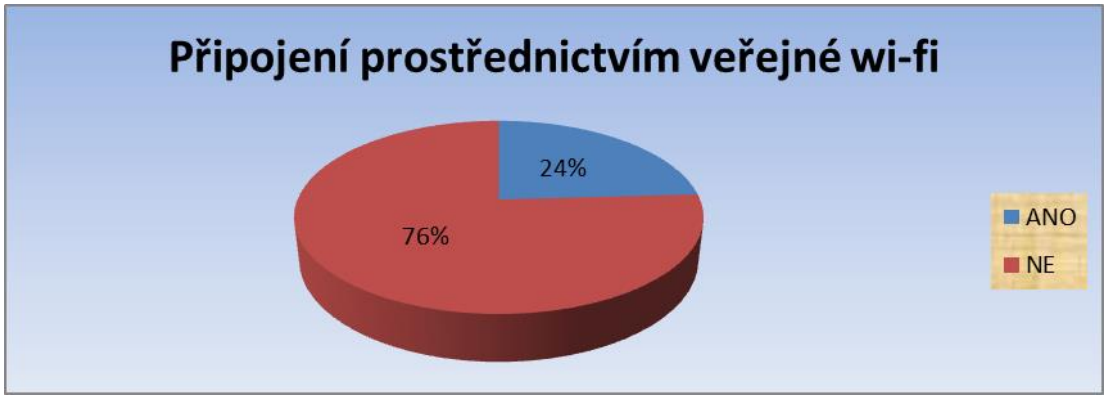
Zdroj: Vlastní zpracování

Veřejná wi-fi síť

Prostřednictvím veřejné wi-fi sítě se naprostá většina respondentů, uživatelů internetového bankovnictví, nepřihlašuje. Celkem 44 respondentů uvedlo, že se prostřednictvím veřejné wi-fi sítě do svého bankovnictví nikdy nepřihlásilo, tedy 76 % dotázaných. Naopak 14 respondentů uvedlo, že se prostřednictvím veřejné wi-fi sítě do bankovnictví přihlásilo, tedy 24 %. Uvedené je patrné v níže uvedeném grafu č. 10,

z kterého vyplývá, že naprostá většina respondentů v tomto směru dodržuje jednu z důležitých zásad bezpečného užívání internetového bankovnictví.

Graf 10 Připojení k bankovnictví prostřednictvím veřejné wi-fi sítě



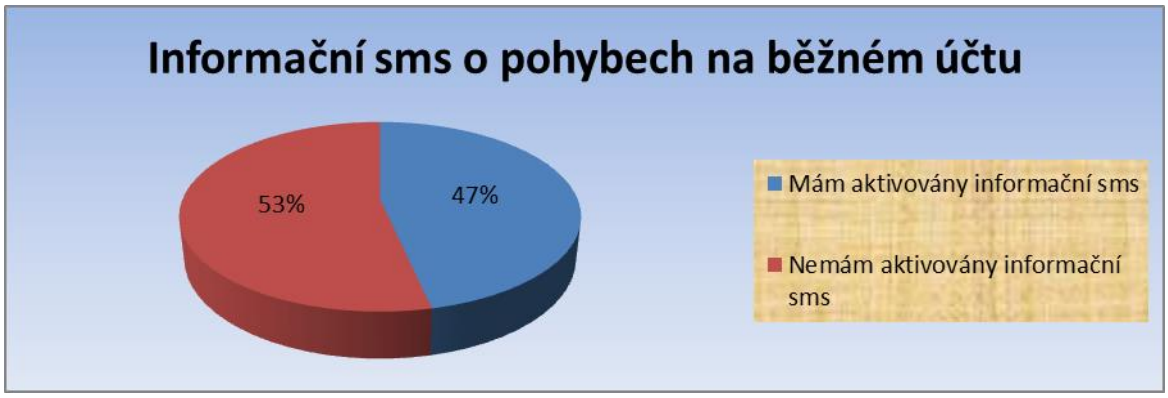
Zdroj: Vlastní zpracování

Přehled o pohybech peněz na běžném účtu

Další, velmi důležitou bezpečnostní zásadou, je mít své finance pod kontrolou. Za tímto účelem si může klient internetového bankovnictví aktivovat informační nebo zůstatkové SMS o pohybech peněžních prostředků na svém běžném účtu. Nadpoloviční většina respondentů uvedla, že nemá aktivovány SMS o pohybech peněžních prostředků na svém účtu, celkem 53 %. Pouze 47 % respondentů dotazníkového šetření uvedlo, že má aktivovány informační sms.

V tomto ohledu většina respondentů nedodržuje výše uvedenou bezpečnostní zásadu, jak je patrné z níže uvedeného grafu č. 11. Důvody, proč toto bankovní službu, která umožňuje okamžitý přehled o pohybech peněz na běžném účtu, není více využívána, je nejspíše poplatek některých bank za tuto službu, nebo prostě nechtějí být obtěžováni častými sms zprávami a důvěřují zabezpečení internetovému bankovnictví.

Graf 11 Informační sms o pohybech na běžném účtu



Zdroj: Vlastní zpracování

Zabezpečení hesla internetového bankovnictví

Chování klienta při používání vybraných bezhotovostních instrumentů při platbách za zboží a služby, z pohledu bezpečnosti, je velmi důležité. Zejména zda dodržuje bezpečnostní zásady a doporučení platebních institucí. Dalším bezpečnostním prvkem, je zabezpečení hesla pro přihlášení do internetového bankovnictví. Celkem 53 % respondentů dotazníkového šetření uvedlo, že nemá žádným způsobem zabezpečené heslo internetového bankovnictví, jak je patrné v grafu č. 12. Zpravidla mají své heslo poznamenané na analogovém dokumentu a uložené doma v zásuvce. Důvody jsou, požadovaná složitost hesla bankami a nemožnost jeho snadného zapamatování klientem banky.

Graf 12 Zabezpečení hesla do internetového bankovnictví

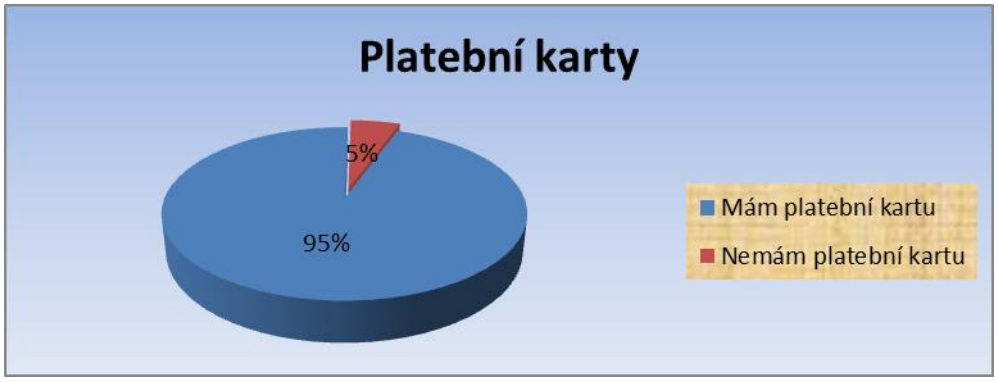
Zdroj: Vlastní zpracování

Platební karty

Platební karta je dnes běžně používaným platebním prostředkem. Kromě výběru hotovosti u bankomatu, který byl u nás v minulosti využíván častěji, dnes slouží k běžnému nákupu v kamenném obchodě a stále častěji i k platbě na internetu. Naprostá většina uživatelů běžného účtu v bance, kromě internetového bankovnictví, má i platební kartu. Celkem 95 % respondentů uvedlo, že má platební kartu, jak je patrné z grafu č. 13.

Tato hodnota značí vysoký stupeň důvěry v tento platební nástroj. Držitelé platebních karet stále častěji používají platební karty k placení v obchodu. To ale neznamená, že riziko zneužití tohoto bezhotovostního platebního prostředku neexistuje. Dále se přesvědčíme, zda si tato rizika držitelé platebních karet uvědomují a vědí jak jim předcházet.

Graf 13 Platební karty

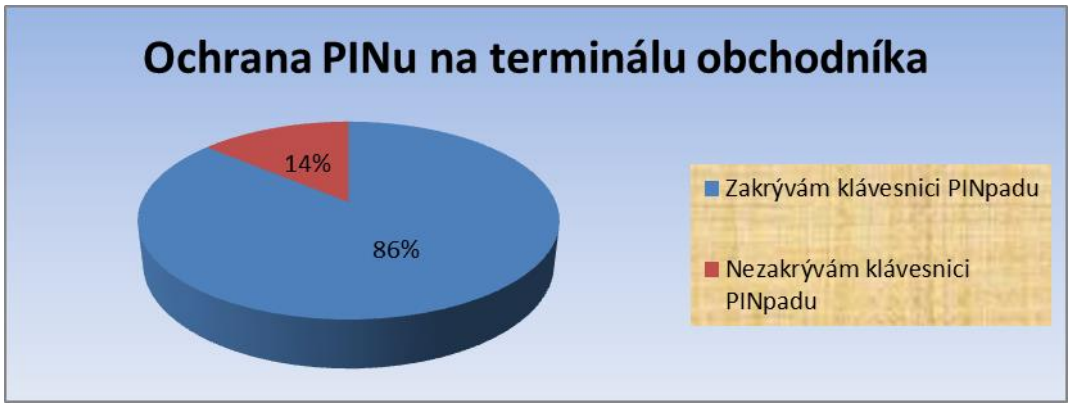


Zdroj: Vlastní zpracování

Ochrana PINu platební karty

V teoretické části byl uveden v kapitole 3.5.4 experiment, zabývající se autorizací platby kartou na terminálu obchodníka. Zaměřený byl na riziko odpozorování PINu při jeho zadávání na PINpadu. Zjištěním bylo, že toto riziko je vysoké, bez zakrytého PINpadu byla 80% úspěšnost odpozorování PINu. Dalším dílčím cílem dotazníkového šetření je ověření, zda si toto riziko držitelé platebních karet uvědomují, a svůj PIN platební karty při jeho zadávání na PINpadu terminálu obchodníka, nebo při výběru hotovosti u bankomatu nějakým způsobem chrání.

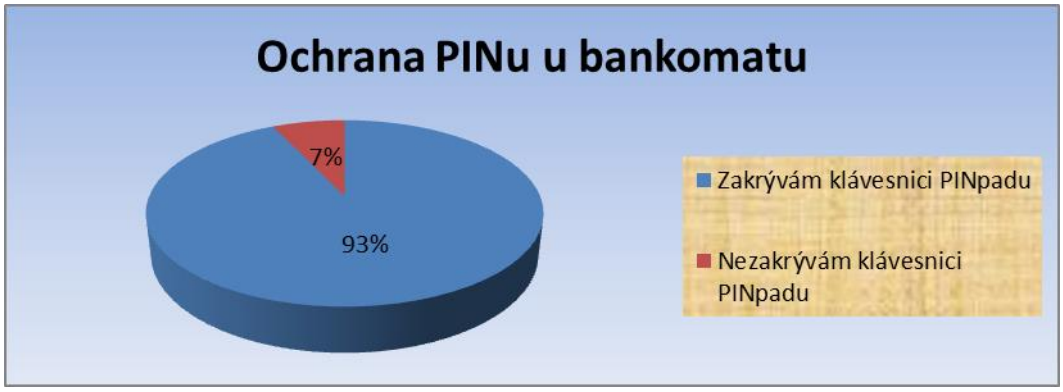
Graf 14 Ochrana PINu u obchodníka



Zdroj: Vlastní zpracování

Z výše uvedeného grafického zpracování je patrné, že naprostá většina respondentů, se při placení kartou u obchodníka chová obezřetně, PIN své platební karty chrání. Celkem 86 % dotázaných uvedlo, že při zadávání PINu karty na číselníku platebního terminálu, tento zakrývají, z důvodu zamezení odpozorování svého PINu.

Graf 15 Ochrana PINu u bankomatu



Zdroj: Vlastní zpracování

Jak již bylo uvedeno v teoretické části, větší riziko podvodného jednání čeká na držitele platební karty u bankomatu, např. riziko skimmingu. I zde je proto na místě, svůj PIN platební karty chránit. Z výše uvedené vizualizace v podobě grafu č. 15 je patrné, že respondenti při výběru hotovosti z bankomatu svůj PIN chrání ještě více, než při platbě u obchodníka. Celkem 93 % dotazovaných uvedlo, že při zadávání PINu karty na číselníku bankomatu, tento zakrývají, aby zamezili případnému odpozorování PINu platební karty podvodníkem.

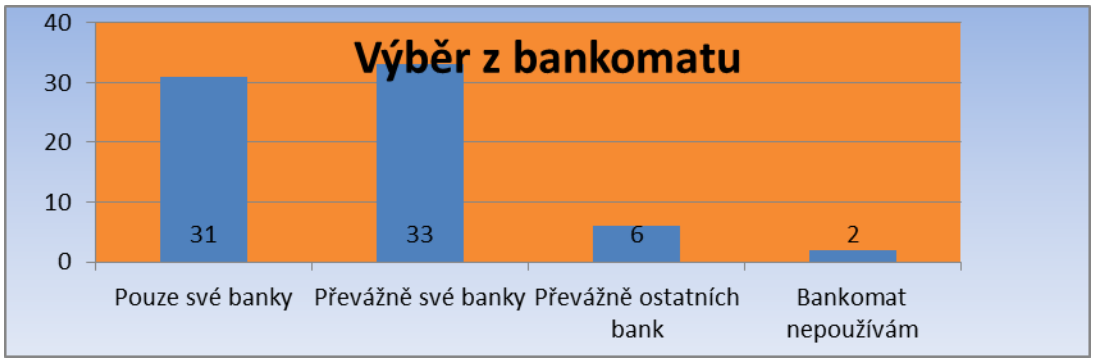
Dalším zjištěním tohoto šetření je, že pouze 2 respondenti ze 72, kteří uvedli držení platební karty, nosí u sebe zapsaný PIN karty. Tedy naprostá většina respondentů, celkem 70 si PIN karty pamatuje.

Z výše uvedeného je patrné, že se respondenti při zadávání PINu karty chovají obezřetně, a PIN nějakým způsobem chrání. Tímto výrazně snižují riziko, že se stanou obětí podvodu. Zvláště opatrně se chovají, při výběru hotovosti u bankomatu, kde na ně čeká největší nebezpečí, které si většinově uvědomují.

Výběr hotovosti u bankomatu

Z níže uvedeného grafu č. 16 je patrné, že nadpoloviční většina respondentů uvedla, že občas vybírá hotovost z bankomatu cizí banky a sedm respondentů uvedlo, že vybírá hotovost převážně z bankomatu ostatních bank. Vzhledem k tomu, že banky používají různé typy bankomatových zařízení, toto představuje určité riziko pro klienta. Z pohledu bezpečného provádění peněžních operací u bankomatu, klient nemusí vědět, jak má daný bankomat vypadat. Které zařízení k němu patří, jako originální příslušenství a které bylo nainstalováno podvodníkem. Vzhledem k tomu, že se případy skimmingu neustále stávají, je evidentní, že odhalení takového zařízení není snadné.

Graf 16 Výběr hotovosti z bankomatu



Zdroj: Vlastní zpracování

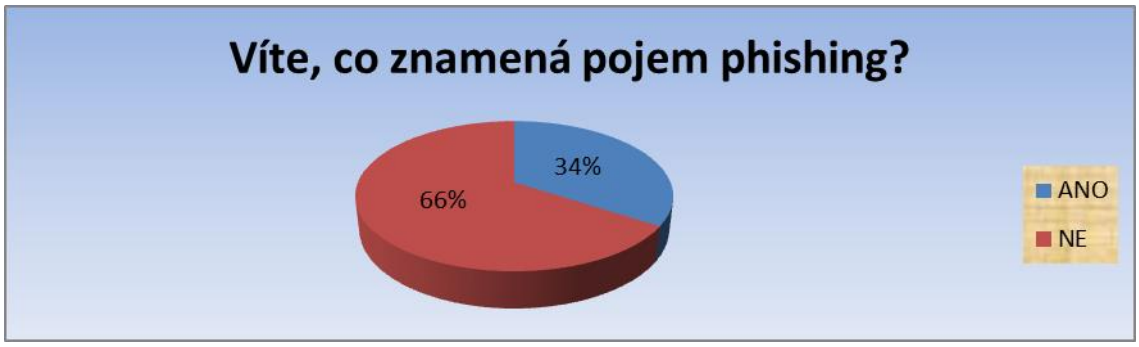
4.1.3 Ohrožení bezhotovostních instrumentů a povědomí klientů

V této podkapitole budou vyhodnoceny výsledky dotazníkového šetření, v oblasti povědomí uživatelů internetového bankovnictví a držitelů platebních karet o možných rizicích, které ohrožují tyto bezhotovostní platební instrumenty.

Dalším dílčím cílem šetření je ověření znalostí respondentů o možných ohroženích bezhotovostních platebních instrumentů, jejich povědomí o druzích útoků a vlastní zkušenosti, kdy se sami ve svém bezprostředním okolí setkali s podvodným jednáním v oblasti bezhotovostního platebního styku. Toto povědomí má vliv na jejich chování, myšleno dodržování základních bezpečnostních zásad, při bezhotovostním placení u obchodníka, a výběru hotovosti u bankomatu.

V závěru dotazníku byly otázky zaměřené na znalosti častých internetových podvodů phisingu a pharmingu. Celkem 50 respondentů uvedlo, že neví co pojem phishing znamená, což je 66 % dotazovaných. Naopak pouze 26 respondentů, což je 34 % dotazovaných, uvedlo, že ví, co tento pojem znamená. Uvedené je patrné z grafu č. 17.

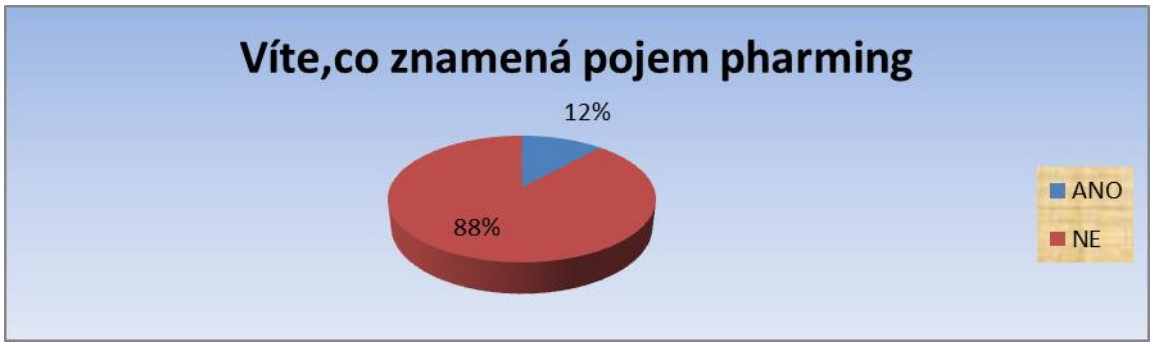
Graf 17 Phishing



Zdroj: Vlastní zpracování

Na otázku, co znamená pharming, odpovědělo celkem 67 respondentů uvedlo, že neví, co pojem pharming znamená, tedy 88 %. Naopak pouze 9 respondentů uvedlo, že ví, co tento pojem znamená, tedy pouze 12 % dotazovaných, viz graf č. 17.

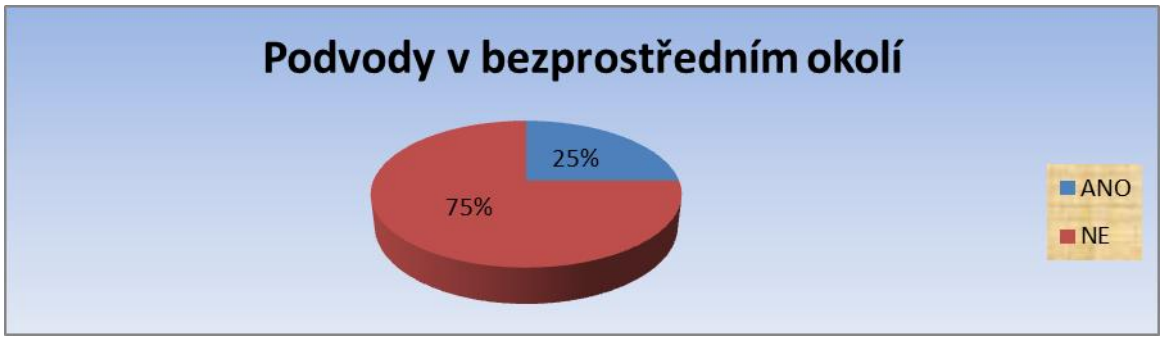
Graf 18 Pharming



Zdroj: Vlastní zpracování

Ve svém bezprostředním okolí se s podvodním jednáním v oblasti internetového bankovnictví setkal každý čtvrtý dotazovaný. Celkem 75 % dotazovaných uvedlo, že se s kriminalitou ve zkoumané oblasti nesetkalo, viz graf č. 19.

Graf 19 Podvody v bezprostředním okolí



Zdroj: Vlastní zpracování

4.1.4 Vyhodnocení dotazníkového šetření

Dotazníkové šetření bylo zaměřeno na využívání služeb internetového bankovnictví a platebních karet. Byla zkoumána četnost jejich využití a způsob chování respondentů, při realizaci tohoto bezhotovostního způsobu platby. Průzkum, byl zaměřen zejména na dodržování základních bezpečnostních zásad a doporučení finančních institucí, neboť chování klienta je velmi důležitý článek v procesu bezhotovostních plateb z pohledu zajištění jeho bezpečnosti.

Výběrový soubor byl z pohledu pohlaví vyvážený, co se týká věku respondentů, bylo dotazníkové zkoumání zaměřeno spíše na starší a z pohledu životních zkušeností tu zkušenější část populace. Z pohledu stupně dosaženého vzdělání, byli v statistickém souboru většinou zastoupeni respondenti s úplným středním vzděláním a vyšším stupněm. Uvedené faktory mají vliv na chování klienta při nakupování, vyšší povědomí o možných rizicích a způsobu ochrany proti podvodníkům, což se nepotvrdilo zcela.

Co se týká vyhodnocení otázek z okruhu internetového bankovnictví, je z výsledků dotazníkového šetření patrné, že čtyři z pěti majitelů běžného účtu mají internetové bankovnictví zřízeno a aktivně ho používají. Frekvence jeho využití je častá až velmi častá. Stále nejvíce jeho uživatelů, se do svého bankovnictví přihlašuje ze svého počítače, z pohodlí svého domova. Přesto počet uživatelů internetového bankovnictví, kteří se připojují prostřednictvím chytrého telefonu, nebo tabletu není zanedbatelný. Naprostá většina respondentů používá softwarovou ochranu svého komunikačního zařízení. Vzhledem k počtu uživatelů internetového bankovnictví a četnosti jeho používání dosvědčuje, že tomuto způsobu bezhotovostního placení lidé důvěřují a nebojí se ho využívat.

Z odpovědí na otázky z okruhu týkajícího se platebních karet je patrné, že držení platební karty je dnes samozřejmostí. Při platbě platební kartou nebo při výběru hotovosti z bankomatu, se klienti chovají obezřetně a naprostá většina chrání PIN karty. Vzhledem k tomu, že většina držitelů alespoň občas vybírá hotovost z cizího bankomatu, než své banky, je na místě zvýšené riziko, že vzhledem k většímu typu bankomatů, nepozná případnou instalaci skimmovacího zařízení na tento bankomat podvodníkem.

Možným řešením problému je v současnosti, kdy mnoho lidí má po ruce chytrý telefon s kamerou, vytvoření aplikace, která po vyfotografování bankomatu dokáže vyhodnotit, že na bankomat bylo nainstalováno neautentizované zařízení a zaslat zprávu provozovateli bankomatu o možném zásahu do tohoto zařízení. Tímto krokem, by mohli být do kontrolního mechanizmu zahrnuti i klienti banky.

Vyhodnocení otázek z okruhu znalostí vybraných způsobů kybernetických útoků podvodníků ukazuje mezery ve znalostech možných ohrožení, při používání sledovaných bezhotovostních platebních instrumentů. To odhaluje, že není vhodné tyto útoky tajit, ale pokud možno co nejvíce a včas o nich informovat. Veřejnost více vzdělávat, zejména o způsobu ochrany proti těmto podvodným jednáním. Vzhledem k počtu respondentů, kteří se ve svém okolí setkali s podvodným jednání, je evidentní, že toto riziko je reálné a ohrožuje peněžní prostředky každého z nás. Na místě je tedy větší zapojení klientů bank do osvěty a samovzdělávání. Možným řešením je např. e-learning v rámci aplikace internetového bankovnictví nebo větší investice do projektů v oblasti prevence a předcházení finanční kriminalitě.

4.2 Rizika bezhotovostního platebního styku

Z pohledu realizace bezhotovostního platebního styku, v bance probíhá řada procesů, při kterých podstupuje rizika. Tato rizika nelze zcela eliminovat a proto je potřeba je systémově řítit. Platební styk se s využíváním moderních technologií stává propracovanějším a mnohem rychlejším. To klade zvýšené nároky na zabezpečení prováděných transakcí. Přibývají útoky na bankovní účty klientů bank prostřednictvím elektronického bankovnictví nebo zneužití platebních karet.

Dle sdružení spotřebitelů lze dělit útoky na bankovní účty na **technické** a **transakční**. S využitím moderních technologií a znalostí dochází ke zneužití citlivých údajů a k útoku na platební prostředek.

Nejčastěji se vyskytující útoky

Skrytá kamera - prostřednictvím skryté kamery, útočník získává PIN. Ke skrytému nahrávání lze využít i mobilní telefon. Tato metoda je používána v kombinaci se skimmingem nebo při platbě u obchodníka.

Dotekové senzory – instalované na klávesnici bankomatu, za účelem získání PINu podvodníkem.

Padělky platebních karet – po získání citlivý dat platební karty podvodníci urychleně vyrobí, v řádu několika minut, padělek karty, který okamžitě zneužijí k podvodu. Zařízení,

které slouží k výrobě padělků, může mít velikost cestovního kufříku. Na padělání platebních karet se podílejí organizované skupiny zločinců z celého světa.

Skimming – pod tímto pojmem je označováno nezákonné jednání, kdy podvodníci zkopírují data platebních karet z magnetického proužku karty oprávněného držitele, a bez jeho vědomí data zkopírují na padělek platební karty. Se skimmingem se nejčastěji můžeme setkat u bankomatu nebo u obchodníka, kde nepoctivý zaměstnanec uvedená data zkopíruje. Nejčastěji se tak děje v barech, restauracích, čerpacích stanicích nebo hotelech.

Útoky prostřednictvím internetu – dochází ke zneužití platební karty nebo peněz na bankovním účtu. Internetovými útoky jsou ohroženy i databáze obchodníků.

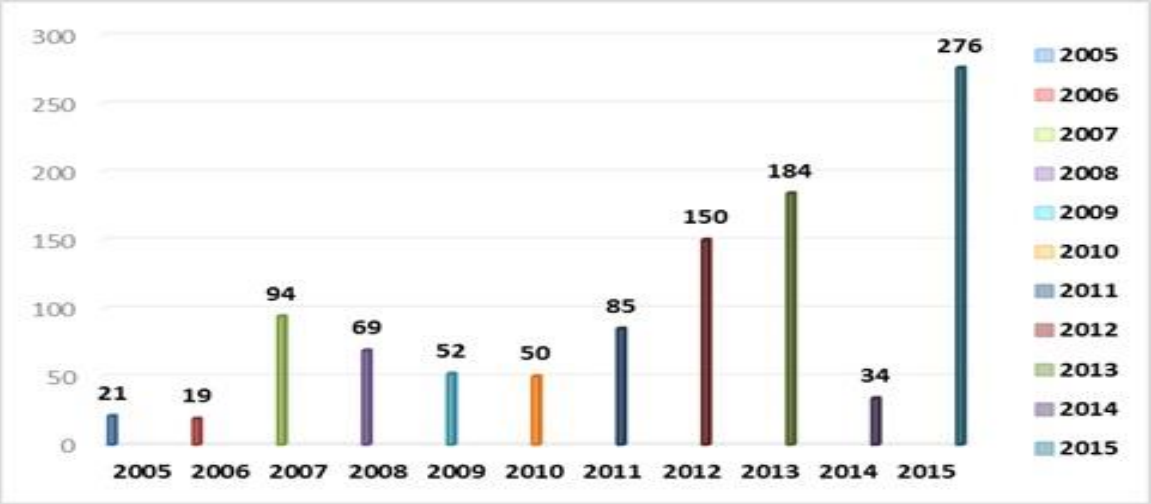
Phishing – je podvod, kdy útočník získá citlivé údaje od uživatele platebního prostředku. Toto je provedeno prostřednictvím e-mailu, uživatel je vyzván k navštívení podvržené stránky, která se tváří jako stránka důvěryhodné instituce, kde zadá své důvěrné informace do formuláře. Informace mohou být následně zneužity podvodníkem k neoprávněnému přístupu.

Pharming - je podvod, kdy uživatel je automaticky přesměrován na internetovou stránku útočníka, která je věrnou napodobeninou bankovní stránky. Ty slouží pro získání přihlašovacích údajů nebo slouží jako zprostředkovatel mezi útočníkem a bankou klienta, přeposílá autorizační údaje a manipuluje s informacemi o provedené transakci. Tato podvodná metoda má dvě varianty, v první je napadán DNS (Domeain Name System), což je systém doménových jmen, který zajišťuje převody doménových jmen a IP adres, což jsou čísla, která identifikují síťové rozhraní v internetu. Uživatel internetového bankovnictví zadá stránku své banky, nedojde ale k jejímu správnému překladu do IP adresy, ale na adresu, kterou zadali podvodníci. Druhá varianta je ta, že podvodníci napadají přímo počítač uživatele, kdy se snaží o zapsání jejich www stránky a domény bankovnictví do host souboru, který pracuje v operačním systému domácího počítače.

Krádež karty – v době, než držitel platební karty zjistí a nahlásí krádež karty, může zloděj zneužít kartu. V případě, že zloděj zná PIN, může získat finanční prostředky výběrem z bankomatu. Pokud ho nezná, může kartu zneužít k neoprávněnému nákupu u obchodníka.

Spyware – je program, který pracuje v počítači uživatele, bez jeho vědomí. Jeho úkolem je sběr informací o uživateli. Do počítače se dostal v podobě trojského koně, což je škodlivý kód přibalený k jinému programu.

Graf 20 Statistický přehled skimmingů v ČR



Zdroj: www.policie.cz

Dalším rizikem, které přináší bezhotovostní způsob placení, je riziko zneužití informací. Prostřednictvím prováděných bezhotovostních plateb lze zjistit pobyt držitele platebního prostředku, jeho pohyb, kde a co nakupuje, trvalé platby, tedy odhalit jeho majetkové poměry. Z opačného úhlu pohledu lze tyto informace využít, pro odhalení a dopadení zločinců. Z uvedeného vyplývá, že zabezpečení informačních technologií musí být na takové úrovni, aby se zamezilo útokům na peněžní prostředky klientů bank a nemohlo dojít ke zneužití informací ke spáchání podvodného jednání.

4.3 Internetové bankovnictví

Za účelem zjištění situace v oblasti zabezpečení internetového bankovnictví, byly u čtyřech vybraných bank zřízeny čtyři běžné účty, a k nim sjednány služby přímého bankovnictví. Pro komunikaci s bankami bylo standardem 128 bitové šifrování s využitím technologie SSL. Na internetových stránkách bank byly informace a návody pro bezpečné používání služeb přímého bankovnictví. Všechny hodnocené banky umožnili přístup k běžnému účtu i prostřednictvím aplikace v chytrém telefonu.

Přihlášení do internetového bankovnictví

U dvou sledovaných bank, se přihlášení do internetového bankovnictví realizuje prostřednictvím klientského čísla a hesla. U třetí sledované banky je nepovinná doplňková možnost nastavení přihlašovací sms zprávy. Ve čtvrté sledované bance je pro úspěšné přihlášení nutné zadání přihlašovacího jednorázového kódu, zaslaného prostřednictvím sms zprávy.

Provádění transakcí

U všech čtyřech bank je nutné pro provedení platby zadání časově omezeného kódu z potvrzovací sms zprávy. Výjimku tvoří dříve uložená a uvedeným kódem potvrzená čísla bankovních účtů, na které lze posílat peníze ze svého účtu již bez nutnosti opětovného zadání potvrzovacího kódu.

Informace o peněžních pohybech a zůstatcích na běžném účtu, všechny uvedené banky poskytují prostřednictvím sms zpráv, nebo e-mailu. Přehledy o pohybech je možné sledovat i prostřednictvím aplikace v chytrém telefonu.

Bezpečnost komunikačních kanálů

Komunikace s bankou probíhá šifrovaně, informace o tom, jak komunikace probíhá a jak má vypadat jsou uvedeny na webových stránkách bank. Zejména jak má vypadat adresní řádek, URL (Uniform Resource Locator), a informace o certifikovaném zabezpečení. Pro komunikaci s bankou je použit certifikát webu banky, který byl bance vydán důvěryhodnou certifikační autoritou, čímž je zabezpečeno, že citlivé informace nemohou být sledovány a pozměněny neoprávněnou osobou.

Informace

Veškeré informace a upozorněn zejména v oblasti bezpečnosti, na případy podvodných jednání, banky zasílají prostřednictvím aplikace internetového bankovnictví, pro které je nutné přihlášení klienta.

Bezpečnostní politika

Sledované banky měli na svých webových stránkách dostupné manuály k internetovému bankovnictví, podmínky jeho užívání, kontakty na příslušné oddělení, které řeší podezřelé události zaznamenané v internetovém bankovnictví a postupy v případě mimořádné události. Dostupné jsou též základní informace o nastavení bezpečnostní politiky banky a, velmi důležitým prvkem je též dostupné desatero, ve kterém jsou uvedena základní bezpečnostní pravidla, které je, při užívání bezhotovostních platebních instrumentů, nutné dodržovat.

Důležitým prvkem je chování klienta při používání služeb přímého bankovnictví. Možným způsobem, který by přispěl ke zvýšení bezpečnostní gramotnosti klientů, je zavedení e-learningových kurzů v oblasti bezpečného užívání bezhotovostních platebních instrumentů. E-learningové kurzy by mohly být přístupné buď na webových stránkách banky, nebo v rámci internetového bankovnictví.

4.4 Bezpečnostní prvky v praxi

4.4.1 Bezpečnost PINu

V této kapitole jsou zpracovány výstupy šetření, které proběhlo v období od 01. listopadu 2016 do 15. ledna 2017 a to v okresech Děčín, Ústí nad Labem a Teplice. Cílem terénního šetření bylo ověření, s využitím empirické metody pozorování, v jaké míře obchodníci využívají dostupné bezpečnostní prvky, zabraňující zneužití bezhotovostních peněžních prostředků svých zákazníků.

V rámci tohoto šetření byl průzkum zrealizován u celkem 64 obchodníků. Pro účely hlubší analýzy nasbíraných dat, byly obchodníci rozdělení do dvou kategorií, a to podle kritéria velikosti prodejní plochy. Malé obchody s velikostí prodejní plochy do 200 metrů čtverečních a velké obchody s prodejní plochou nad 200 metrů čtverečních.

Rozsah sledovaného souboru byl tedy 64 jednotek, které byly do pozorování zahrnuty prostým náhodným výběrem. Reprezentativnost a rozsah vybraného vzorku pro účely

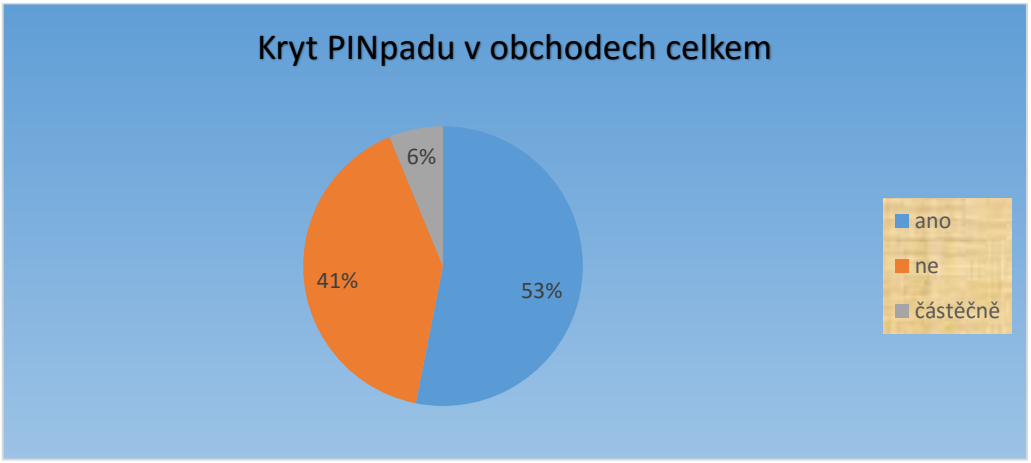
zkoumání využití bezpečnostního prvku platebních karet, je pro vytýčené cíle a účely na dostatečné úrovni.

Cílem pozorování bylo zjištění, v jaké míře je používaný bezpečnostní prvek ochranného krytu PINpadu, který zabraňuje odpozorování PINu platební karty neoprávněnou osobou. Zachycení skutečného stavu, popis a vysvětlení zjištění a kvantifikace výše rizika pro držitele platebních karet. Pro stanovení rizika úspěšného odpozorování PINu platební karty, budou využity analogicky výstupy experimentu Masarykovi univerzity, uvedeného v kapitole 3.5.4 na straně 40.

Obchody celkem

Realizací pozorování využití bezpečnostního prvku platebních karet, ochranného krytu PINpadu, u obchodníků bylo zjištěno, že z celkem 64 obchodů mělo platební terminál s ochranným krytem PINpadu celkem 34 obchodů, bez uvedeného krytu bylo 26 obchodů a ve 4 případech měly obchodníci ochranné kryty na PINpadech svých platebních terminálů jen částečně. Částečné vybavení platebních terminálů krytkami se ve všech případech týkalo velkých obchodů. Dle typu platebního terminálu se jednalo o stejný model a výrobce, pouze krytky byly odnímatelné a tak postupem času došlo u části platebních terminálů k jejich ztrátě.

Graf 21 Kryt PINpadu v obchodech celkem

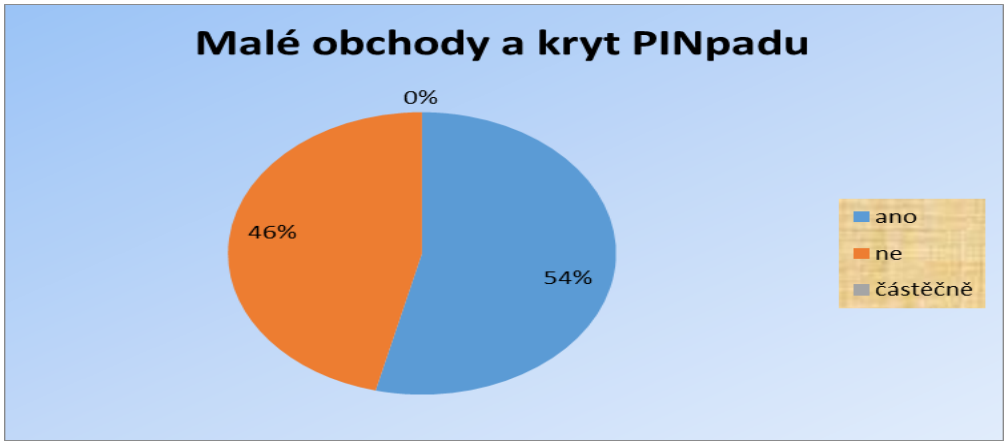


Zdroj: Vlastní zpracování

Malé obchody

V případě malých obchodů, mělo svůj platební terminál opatřený ochranným krytem PINpadu celkem 14 obchodů, což činilo 54 % ze sledovaného souboru. Bez uvedeného krytu bylo 12 obchodů, což představuje 46 % obchodů. Uvedené si můžeme ukázat vizuálně v podobě grafu č. 20.

Graf 22 Malé obchody a ochranný kryt PINpadu

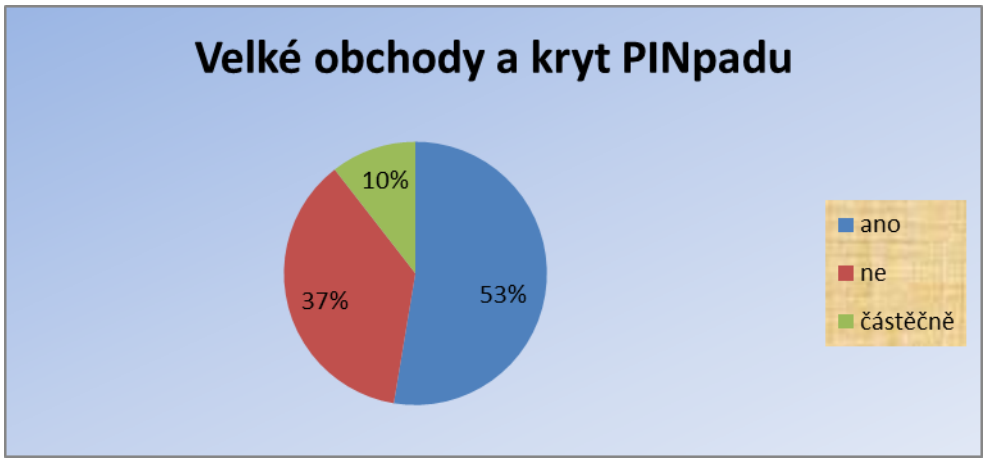


Zdroj: Vlastní zpracování

Velké obchody

Pozorováním, realizovaným ve velkých obchodech, bylo zjištěno, že v celkem 20 případech pozorování měli obchody na svých platebních terminálech nainstalovány ochranné kryty PINpadu, což představuje 53 %. U 14 obchodníků bylo zjištěno, že své terminály nemají opatřeny ochranným krytem PINpadu a ve 4 případech bylo zjištěno, že ochranné kryty má část PINpadů, jak je již uvedeno výše. I u velkých obchodů byla situace obdobná jako u malých obchodů a podíl obchodů vybavených ochranným krytem PINpadu byl obdobný, 54 % ku 53 %. Uvedené znázorňuje ve vizuální podobě graf č. 21 níže.

Graf 23 Velké obchody a ochranný kryt PINpadu



Zdroj: Vlastní zpracování

Riziko odpozorování PINu v praxi

S odkazem na výstupy experimentu provedeném na Fakultě informatiky Masarykovi univerzity, kde bylo zjištěno, že u platebních terminálů bez ochranného krytu PINpadu bylo úspěšně odpozorováno pozorovatelem 80 % PINů a u platebních terminálů opatřených ochranným krytem PINpadu bylo úspěšně odpozorováno 35,5 % PINů, můžeme analogicky odvodit současnou výši rizika úspěšného odpozorování PINu. Pro výpočet použijeme níže uvedený vzorec. Kde výše rizika úspěšného odpozorování PINu, vyjádřena procentně, v malých obchodech značíme M a ve velkých obchodech V.

Pro výpočet rizika úspěšného odpozorování PINu platební karty byl použit vzorec, který je tvořen sumou podílů ochodů násobených rizikem odpozorování, vyjádřeného úspěšným odpozorováním PINu v procentech citovaného experimentu Masarykovi univerzity na straně 40, dle vybavenosti krytem, bez krytu nebo částečně. V případě částečného vybavení krytem, byl použit vážený průměr rizika.

$$\text{Riziko M} = \frac{54}{100} \text{ x } 35{,}5\ \% + \frac{46}{100} \text{ x } 80\ \% = 57{,}97\ \%$$

$$\text{Riziko V} = \frac{53}{100} \text{ x } 35{,}5\ \% + \frac{37}{100} \text{ x } 80\ \% + \frac{10}{100} \text{ x } \left(\frac{35.5\%+80\%}{2}\right) = 54.19\ \%$$

$$\text{Riziko C} = \frac{53}{100} \text{ x } 35{,}5\% + \frac{41}{100} \text{ x } 80\% + \frac{6}{100} \text{ x } \left(\frac{35{,}5\%+80\%}{2}\right) = 55{,}08\%$$

Z výpočtu výše rizika je patrné, že o něco vyšší riziko úspěšného odpozorování PINu je v malých obchodech, a to 57,97 %. Ve velkých obchodech je riziko odpozorování 54,19 %.

Z pohledu držitele platební karty a jeho zájmu uchovat tajemství PINu, je jeho zadávání na terminálu obchodníka vysoce rizikové. Můžeme si logicky vyvodit závěr, že vzhledem k pohybu dalších zákazníků v blízkosti platebního terminálu, je zadávání PINu v obchodě rizikovější, než jeho zadávání u bankomatu, kde je držitel karty obezřetnější, z pohledu možného odpozorování PINu platební karty.

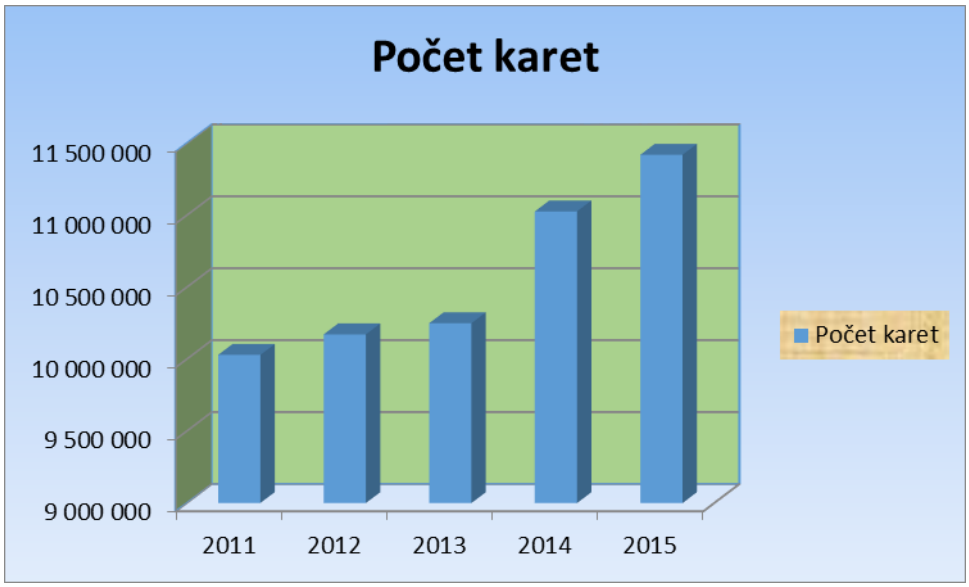
Výsledky dílčího šetření vybraného bezpečnostního prvku, krytu PINpadu platebního terminálu, nejsou nijak povzbudivé. Vidíme, že obchodníci z pohledu bezpečnosti mají co dohánět. Platební terminály jsou výhradně pod kontrolou obchodníků, zajištění odpovídajícího servisu a vybavenosti PINpadů terminálů, a tím zvýšení úrovně bezpečnosti karet, mohou tedy ovlivnit obchodníci.

4.4.2 **Bezpečnostní situace v oblasti platebních karet v České republice**

Podvody s platebními kartami

Tato kapitola pojednává o statistických přehledech podvodných jednání, kde hlavní úlohu hrají platební karty. Za účelem porovnání trendů v této oblasti byl zpracován statistický přehled. Zdrojem vybraných statistických údajů byla data Policie České republiky a Sdružení pro bankovní karty. Cílem bude ověření bezpečnosti platebních karet. Pro účely šetření úrovně zabezpečení budou pro vyhodnocení použita kritéria, podíl podvodů na celkovém počtu vydaných platebních karet, objem a počet transakcí prostřednictvím platebních karet.

Graf 24 Platební karty v České republice



Zdroj: Sdružení pro bankovní karty, vlastní úprava

Jak je patrné z grafu č. 22, tak platební karty jsou v České republice zcela běžným platebním prostředkem, vzhledem k počtu obyvatel. Je běžné, že klient banky má více než jednu platební kartu, ať už v podobě kreditní nebo debetní platební karty. Segment trhu platebních karet má stále růstový potenciál. Lidé se nebojí používat platební karty i k drobným nákupům, jak je patrné z vizuálního vyjádření v podobě grafu č. 23. Z uvedeného grafu je patrný výraznější nárůst počtu transakcí, realizovaných prostřednictvím platebních karet, doprovázený nižším nárůstem objemu těchto transakcí. To znamená, že průměrná výše částky, kterou zákazník svou platební kartou zaplatí, se snižuje. Uvedené má vliv na snížení rizika odpozorování PINu platební karty, neboť při drobných platbách není u bezkontaktních karet nutné zadání PINu.

Graf 25 Transakce prostřednictvím platebních karet

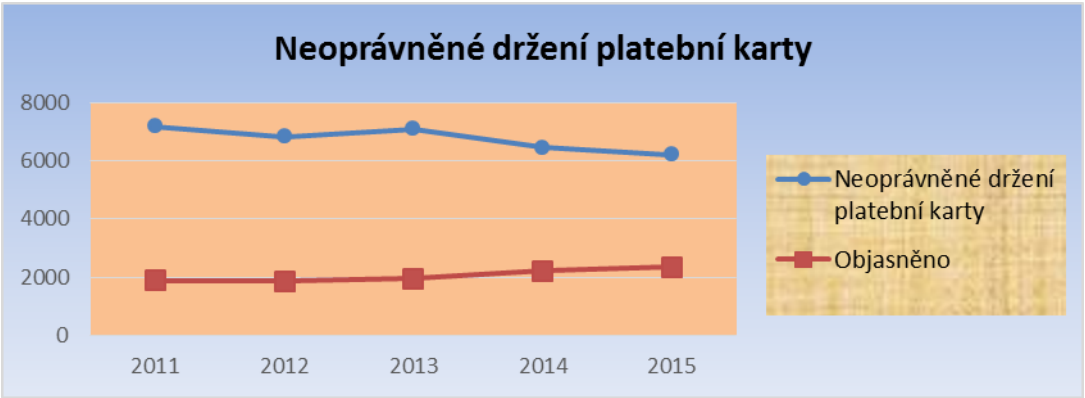
Zdroj: Sdružení pro bankovní karty, vlastní úprava

Neoprávněné držení platební karty

Představu o situaci, jak to ve skutečnosti vypadá s bezpečností platebních karet v České republice a možného vývoje rizika držitelů platebních karet, že se stanou obětí podvodného jednání, si můžeme udělat ve vizuálním vyjádření z grafu č. 24. V grafu jsou znázorněny počty případů neoprávněného držení platební karty, z uvedeného je patrný pokles těchto případů v posledních pěti letech.

Zároveň se Policii České republiky v uvedeném období dařilo objasňovat podvody s platebními kartami. Z uvedeného grafu je patrný nárůst objasněných trestných činů neoprávněného držení platebních karet. S nárůstem objasněnosti, narostl i počet trestně stíhaných podvodníků s platebními kartami, kdy v roce 2011 to bylo 1225 stíhaných osob a v roce 2015 to bylo už 1553 stíhaných osob. Tyto statistické údaje vypovídají o zlepšující se bezpečnostní situaci v oblasti platebních karet. Tento, pro držitele platebních karet, pozitivní trend si můžeme vysvětlit pomocí vlivu několika faktorů. Jedním z pozitivních faktorů, mající vliv v oblasti bezpečnosti platebních karet je evidentně lepší práce Policie České republiky a tím nejdůležitějším pak zavádění lepší, čipové technologie platebních karet bankami.

Graf 26 Neoprávněné držení platební karty



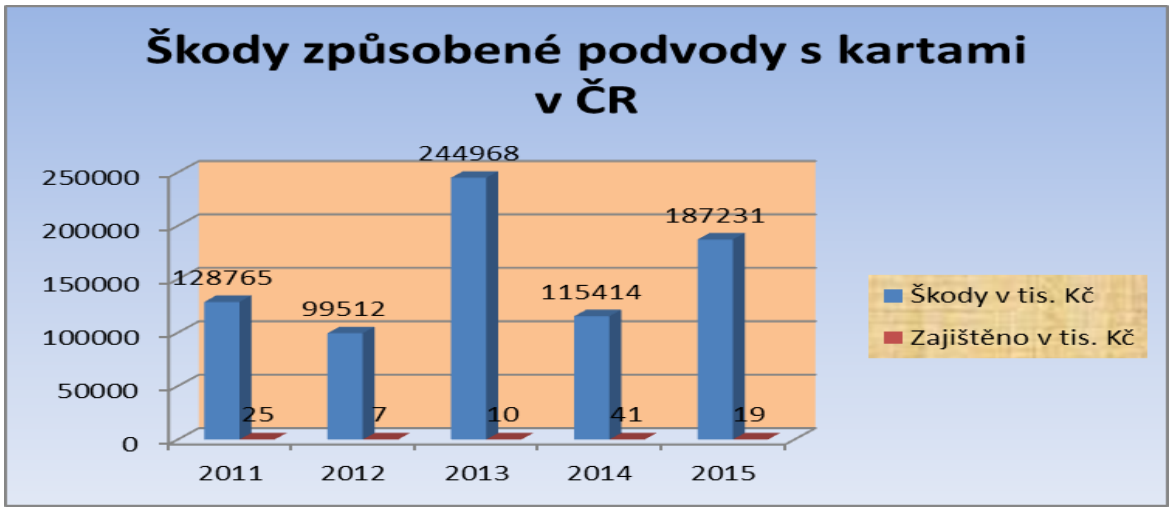
Zdroj: Policie České republiky, vlastní úprava

Škody způsobené podvodníky

Škody způsobené podvodníky držitelům platebních karet nejsou v absolutní částce nikoli nepatrné, o čemž se můžeme přesvědčit z grafu č. 25. Vzhledem k počtu a objemu transakcí realizovaných prostřednictvím platebních karet jsou na přijatelné úrovni. V roce 2015 bylo prostřednictvím platebních karet realizováno 789 milionů transakcí o objemu 409 miliard korun. Škoda způsobená podvodníky byla 187 milionů korun, což je necelé půl promile z objemu transakcí. V tomto kontextu můžeme platební karty považovat za přiměřeně bezpečný platební prostředek.

Negativní zprávou je, že se orgánům činným v trestním řízení v České republice nedaří zajistit peněžní prostředky, získané podvodníky s platebními kartami. Tato nízká úspěšnost je způsobená zejména tím, že tyto podvody jsou mezinárodně organizovány a odcizené peníze končí v krátkém čase v zahraničí. Což jsou bariéry, díky kterým není Policie České republiky příliš efektivní. V uvedeném období se úspěšnost policie, měřeno výší zajištěných peněžních prostředků, pohybuje od 7 do 41 tisíc Kč v kalendářním roce. Vzhledem k výši škody, kterou podvodníci způsobili, je výše zajištěných peněz policií zanedbatelná.

Graf 27 Škody způsobené podvodníky



Zdroj: Policie České republiky, vlastní úprava

Pachatelé podvodů

Motiv podvodníků neboli objekt podvodu je jasný, zisk finančního prospěchu. Ale kdo je takovým typickým podvodníkem, zda odborně zdatný profesionál, nebo okolnostmi dohnaný náhodný pachatel? Určitou představu si můžeme udělat z policejních statistik kriminality. Z uvedených statistik kriminality vyplývá, že více než polovinu trestně stíhaných osob, které se v České republice dopustily trestného činu neoprávněného držení platební karty, jsou recidivisté. Tedy lidé, kteří jsou za své podvodné jednání v oblasti platebních karet stíháni opakovaně. Lze tedy vyvodit, že se na danou oblast platebních karet specializují. Dalším zajímavým údajem kriminalistických statistik je, že v uvedeném období rostl podíl žen, které se dopustili podvodného jednání v oblasti platebních karet. Což je mimo jiné způsobeno, že něžné pohlaví spíše páchá nenásilnou trestnou činnost, kam patří i podvody s platebními kartami.

Tabulka 1 Neoprávněné držení platební karty

	2011	2012	2013	2014	2015
Celkem spácháno	7181	6822	7093	6450	6215
Objasněno	1874	1852	1948	2214	2352
Recidivisté - počet skutků	1022	838	1128	1349	1396
Stíháno osob	1225	1201	1401	1527	1553
Stíhaní recidivisté	548	522	715	778	869
Ženy	330	363	382	408	395
Škody v tis. Kč	128765	99512	244968	115414	187231
Zajištěno	25	7	10	41	19

Zdroj: Policie České republiky, vlastní úprava

Vyhodnocení bezpečnostní situace v oblasti platebních karet

Dle dostupných údajů o trestné činnosti v oblasti platebních karet, viz tabulka č. 1, lze shrnout, že riziko podvodného jednání je na přijatelné úrovni. V posledních 5-ti letech se situace zlepšuje, dílem úspěšného přechodu na čipovou technologii záznamu dat platebních karet, standardu EMV, a dílem úspěšnější práce v odhalování podvodů s platebními kartami Policií České republiky. Negativem zůstává velmi nízká úspěšnost v zajišťování odcizených peněžních prostředků, vzhledem k celkovým škodám, které podvodníci napáchali, se podaří zajistit jen zlomek odcizených peněz.

5 Výsledky a diskuse

Pokud porovnáme tento výzkum s pracemi ostatních autorů, lze dojít k závěru, že se zabývá podobnými otázkami, zabývajícími se bezpečností bezhotovostních platebních instrumentů. V první řadě pokud jde o rozsah informací k danému tématu, bezpečnostními prvky, které přispívají k vyšší bezpečnosti bezhotovostních platebních nástrojů, vymezení nejvýznamnějších ohrožení a návrhů na vylepšení bezpečnostních opatření, která mohou přispět k dosažen vyšší úrovně zabezpečení vymezených bezhotovostních platebních nástrojů. Lze zde najít informace o aktuálním vývoji a trendu z pohledu bezpečnosti, prostřednictvím kterých lze odvodit rostoucí důvěru uživatelů bezhotovostních platebních instrumentů.

Vyhodnocením výsledků dotazníkového šetření bylo zjištěno, že čtyři z pěti majitelů běžného účtu mají internetové bankovnictví zřízeno a aktivně ho používají. Lidé mají tendenci důvěřovat svému počítači a tak se ke svému bankovnictví přihlašují spíše ze svého domova. Ale počet klientů, kteří se přihlašují prostřednictvím chytrého telefonu, nebo tabletu není zanedbatelný a zejména díky mladší generaci poroste. Připojení těchto zařízení preferují datové připojení, prostřednictvím veřejné wi-fi sítě se tři čtvrtiny lidí, z bezpečnostních důvodů, ke svému bankovnictví nepřipojuje. Vzhledem k podílu uživatelů přímého bankovnictví a četnosti jeho používání lze usoudit, že internetové bankovnictví má důvěru lidí, z pohledu komfortu, který tato služba poskytuje a úrovni zabezpečení, kterou je zajištěna. Lze říci, že lidé se nebojí přímé bankovnictví aktivně používat.

Jedním z důležitých prvků zabezpečení internetového bankovnictví a platebních karet je chování jejich uživatelů. Výstupem dotazníkového šetření bylo zjištění, jak uživatelé vybraných bezhotovostních platebních instrumentů dodržují základní bezpečnostní zásady, a doporučení vydávané bankami.

Dalším důležitým prvkem je zabezpečení komunikačního zařízení. Z celkem 58 dotázaných uvedlo 53, že používá nějaký zabezpečovací program ve svém počítači, ze kterého se přihlašuje do aplikace internetového bankovnictví. Pouze 5 dotázaných žádnou ochranu svého počítače nepoužívá. Je tedy patrné, že naprostá většina uživatelů

internetového bankovnictví používá softwarové zabezpečení svého počítače. Tedy aktivně přispívají k vyšší úrovni zabezpečení bankovnictví.

Šetřením bylo zjištěno, že heslo do svého bankovnictví nemá 53% respondentů žádným způsobem zabezpečeno. Důvodem je požadovaná složitost hesla bankami a nemožnost jeho snadného zapamatování. Své heslo mají zpravidla poznamenané a uložené v zásuvce, což dle odborníků není problém. Z pohledu bezpečnosti je možným vylepšením, mít analogové dokumenty s hesly uloženy v uzamykatelné schránce tak, aby tato citlivá data nemohla být nikým zneužita, např. návštěvou.

Vyhodnocením dílčích výsledků dotazníkového šetření v oblasti znalostí uživatelů internetového bankovnictví v oblasti možných rizik, způsobů kybernetických útoků na internetové bankovnictví, odhalilo mezery ve znalostech a povědomí lidí o těchto ohroženích. Na otázku co pojem phishing, odpovědělo 66% respondentů, že neví, co tento pojem znamená. Na otázku co je pharming, pak odpovědělo 88% dotázaných, že neví co pharming znamená. Vzhledem k tomu, že se každý čtvrtý dotázaný se ve svém okolí setkal s podvodným jednáním v oblasti internetového bankovnictví, je pak tato nevědomost uživatelů o možných ohroženích alarmující. V rámci bezpečnostních politik jednotlivých bank je již řešeno. Informovanost klientů prostřednictvím bezpečných komunikačních kanálů, např. prostřednictvím aplikace elektronického bankovnictví, o aktuálně provedených útocích a způsobu ochrany je zajištěna. Možným návrhem na zlepšení v této oblasti je realizace e-learningových kurzů v oblasti bezpečného užívání přímého bankovnictví. E-learningové kurzy by mohly být přístupné buď na webových stránkách banky, nebo v rámci internetového bankovnictví.

Dílčí šetřením, kde cílem pozorování bylo zjištění, v jaké míře je používaný bezpečnostní prvek ochranného krytu PINpadu na platebních terminálech obchodů. Bylo zrealizováno celkem 64 pozorování. Výsledkem šetření je zjištění, že z celkem 64 obchodů mělo platební terminál s ochranným krytem PINpadu celkem 34 obchodů, bez uvedeného krytu bylo 26 obchodů a ve 4 případech měly obchodníci ochranné kryty na PINpadech svých platebních terminálů jen částečně. Platební terminály jsou výhradně pod kontrolou obchodníků, zajištění odpovídajícího servisu a vybavenosti PINpadů terminálů, a tím

zvýšení úrovně bezpečnosti karet je v gesci obchodníků. Vhodným řešením pro zlepšení situace, jsou pevně instalované kryty PINpadu, které nelze odstranit.

Při platbě kartou v obchodě pak při zadávání PINu zakrývá číselník PINpadu platebního terminálu celkem 86% respondentů. Z uvedeného vyplívá, že si naprostá většina držitelů platebních karet uvědomuje riziko odpozorování PINu platební karty a proto ho nějakým způsobem chrání, kdy tímto výrazně přispívají ke snížení rizika odpozorování PINu.

Vyhodnocením otázky, týkající se výběrů z bankomatu bylo zjištěno, že nadpoloviční většina dotázaných odpověděla, že občas vybírá hotovost z bankomatu cizí banky a sedm respondentů uvedlo, že vybírá hotovost převážně z bankomatu ostatních bank. Lze se domnívat, vzhledem k odbourávání poplatků za běžné transakce a výběry hotovosti z bankomatu, že výběry z bankomatů cizích bank porostou. Vzhledem k tomu, že banky používají různé typy bankomatových zařízení, toto představuje určité riziko pro klienta. Jak má daný bankomat vypadat, které zařízení k němu patří jako originální příslušenství a které bylo nainstalováno podvodníkem, není pro klienta snadné vyhodnotit, vzhledem k tomu, že se případy skimmingu neustále opakují. Vhodným řešením tohoto problému by mohlo být, kdy mnoho lidí má po ruce chytrý telefon s digitální kamerou, vytvoření aplikace, která po vyfotografování bankomatu dokáže vyhodnotit, že na bankomat bylo nainstalováno neautentizované zařízení a zaslat zprávu provozovateli bankomatu o možném zásahu do tohoto zařízení. Tímto krokem, by mohli být do kontrolního mechanizmu zahrnuti i klienti banky.

Vyhodnocením statistických údajů dostupných na webových stránkách Policie ČR a Sdružení pro bankovní karty lze říci, že riziko podvodného jednání v oblasti platebních karet je vzhledem k počtu vydaných karet a objemu transakcí na přijatelné úrovni, kdy činí necelé půl promile z objemu transakcí realizovaných platebními kartami. V období let 2011 až 2015 se bezpečnostní situace v oblasti karet postupně zlepšuje, což je způsobeno přechodem na čipovou technologii a lepší prací policie. Možným řešením na další zlepšení situace může být personální stabilizace policie a zaměření na vyšší zajištění odcizených peněžních prostředků, což vzhledem k mezinárodně organizovaným podvodům není snadný úkol.

6 Závěr

V současnosti je již zcela běžné, že k placení jsou využívány bezhotovostní způsoby platby. Nejčastěji v podobě platby kartou nebo platebním příkazem v internetovém bankovnictví. Ke svému běžnému účtu, vedeném v bance, má naprostá většina uživatelů zřízeny i služby internetového bankovnictví a vydanou platební kartu. Jak vyplývá z výsledků dotazníkového průzkumu, tak internetové bankovnictví má zřízeno 76% uživatelů běžného účtu. Celkem 54% uživatelů internetového bankovnictví ho pak aktivně používá. Platební kartu ke svému účtu má vydanou celkem 95 % uživatelů běžného účtu.

Důvody rostoucí obliby bezhotovostních platebních instrumentů lze odvodit z výsledků dotazníkového šetření a analýzy statistik kriminality zpracovaných Policí České republiky a statistik Sdružení pro bankovní karty. Jedním důvodů obliby je jednoduchost a komfort platebních postupů, kdy své peníze v bance mají její klienti dostupné kdykoli a platbu mohou v případě internetového bankovnictví provést z bezpečí svého domova. V případě platebních karet pak odpadá nutnost mít hotovost u sebe, kdy odpadá riziko krádeže, a samotná platba na platebním terminálu obchodníka zabere pár vteřin.

Vyhodnocením otázek z okruhu znalostí vybraných způsobů kybernetických útoků podvodníků, odhalilo mezery ve znalostech respondentů o možných způsobech ohrožení ze strany podvodníků. Na místě je tedy větší zapojení klientů bank do osvěty a samovzdělávání. Možným řešením je např. e-learning v rámci aplikace internetového bankovnictví, podpořený motivačním benefitem, a větší investice do projektů v oblasti prevence a předcházení finanční kriminalitě.

V segmentu platebních karet je patrný nárůst počtu vydaných karet. Ve sledovaném období, od roku 2011 do roku 2015, počet vydaných karet neustále rostl, z hodnoty 10 030 193 vydaných karet v roce 2011 na hodnotu 11 421 038 vydaných karet v roce 2015, dle dostupných údajů na webu Sdružení pro bankovní karty. Z pohledu zajištění bezpečnosti platebních karet, měřeno počtem evidovaných případů podvodného jednání Policií České republiky, došlo ve sledovaném období k poklesu případů neoprávněného držení platební karty, kdy v roce 2011 to bylo 7181 případů a v roce 2015 pokles na 6215 evidovaných skutků. V roce 2015 bylo prostřednictvím platebních karet provedeno 789

milionů transakcí, jejichž objem dosáhl 409 miliard korun. Škoda, kterou způsobili podvodníci, dosáhla za rok 2015 hodnoty 187 milionů korun, což je necelé půl promile z objemu provedených transakcí kartami v daném roce. Z uvedeného lze dojít k závěru, že placení kartou je bezpečné a riziko podvodu je na přijatelné úrovni. Negativem je, že se dlouhodobě nedaří zajistit peněžní prostředky, získané podvodníky s platebními kartami. Možným způsobem jak zlepšit situaci, je personální stabilizace Policie České republiky, aby bylo snazší zajistit odborníky v dané problematice z vlastních zdrojů.

Ke snížení rizika odpozorování PINu platební karty přispívá bezpečnostní prvek kryt PINpadu platebního terminálu. Šetřením, provedeným pozorováním v obchodech, byly zjištěny nedostatky ve vybavenosti kryty PINpadu. V mnohých případech byl platební terminál původně vybaven odnímatelným krytem PINpadu, který byl později odstraněn. Návrhem na zlepšení je instalace PINpadu s pevně zabudovaným krytem PINpadu, a z pohledu bezpečnosti odpovídající servis stávajících zařízení.

Místem, které je pro držitele platebních karet velmi rizikové, je bankomat. V dotazníkovém šetření uvedla nadpoloviční většina respondentů, že občas nebo převážně vybírá hotovost z bankomatu cizí banky. Jak má daný bankomat vypadat, které zařízení k němu patří jako originální příslušenství a které bylo nainstalováno podvodníkem, není pro klienta snadné vyhodnotit, vzhledem k tomu, že banky používají různé druhy zařízení.

Vhodným řešením tohoto problému by mohlo být vytvoření aplikace pro chytré telefony, která po vyfotografování bankomatu dokáže vyhodnotit, porovnáním s databází, zda na bankomat bylo nainstalováno neautentizované zařízení a zaslat zprávu provozovateli bankomatu o možném zásahu do tohoto zařízení. Tímto krokem, by mohli být do kontrolního mechanizmu zahrnuti i klienti banky.

Přínos této práce je možné spatřovat v tom, že klienti finančních institucí si mohou udělat obrázek o aktuální bezpečnostní situaci v řešené oblasti bezhotovostních platebních instrumentů. Odhaluje dílčí nedostatky platebních postupů, a navrhuje jejich možná vylepšení, která by mohla přispět ke zvýšení úrovně bezpečnosti řešených platebních nástrojů.

7 Seznam použitých zdrojů

Přehled literatury

FRANK, Robert H. a Ben BERNAKE. 2003. *Ekonomie.* 1. vyd. Praha : Grada, 2003. ISBN: 80-247-0471-4.

HARTMANN, Monika E. 2000. *Elektronisches Geld und Geldpolitik eine Analyse der Wechselwirkungen.* Karlsruhe : Univ.-Verl. Karlsruhe, 2000. ISBN:3-937300-31-7.

JÍLEK, Josef. 2013. *Finance v globální ekonomice I. Peníze a platební styk.* 1. vyd. Praha : GRADA Publishing, a.s., 2013. ISBN: 978-880-247-3893-2.

JUŘÍK, Pavel. 2006. *Platební karty velká enciklopedie 1870-2006.* 1. vyd. Praha : Grada Publishing, a.s., 2006. ISBN: 80-247-1381-0.

KALABIS, Zbyněk. 2012. *Základy bankovnictví: bankovní obchody, služby, operace a rizika.* 1. vyd. Brno : BizBooks, 2012. ISBN: 978-80-265-0001-8.

MÁČE, Miroslav. 2006. *Platební styk: klasický a elektronický.* 1. vyd. Praha : Grada Publoshing, 2006. ISBN: 80-247-1725-5.

MATYÁŠ Vašek, Jan KRHOVJÁK a kol. 2007. *Autentyzace uživatelů a autorizace elektronických transakcí: příručka pro managera = User authentication and elektronic transaction authorization: manager' shandbook.* 1. vyd. Praha : TATE International, 2007. ISBN: 978-80-86813-14-1.

MEJSTŘÍK Michal, Magda PEČENÁ a Petr TEPLÝ. 2014. *Bankovnictví v teorii a praxi: Banking in theory and practice.* 1. vyd. Praha : Karolinum, 2014. ISBN: 978-80-246-2870-7.

NOVESKÝ, Ivan a kol. 2009. *Slabikář finanční gramotnosti: učebnice základních 7 modulů finanční gramotnosti.* 1. vyd. Praha : Karolinum, 2009. ISBN: 978-80-254-4207-4.

POLIDAR, Vojtěch a Martin MANDEL. 1999. *Management bank a bankovních obchodů.* 2. upr. vyd. Praha : Ekopress, 1999. ISBN: 80-86119-11-4.

POLOUČEK, Stanislav a kol. 2006. *Bankovnictví.* 1. vyd. Praha : C.H:Beck v Praze, 2006. ISBN: 80-7179-462-7.

PŘÁDKA, Michal a Jan KALA. 2000. *Elektronické bankovnictví.* 1. vyd. Praha : Computer Press, 2000. ISBN: 80-7226-328-5.

RAINA, Vibha Kaw. 2015. *Banking, Financa, and Accourting: Concepts, Methodologies, Tools, And applications.* New Delhi : IGI Global, 2015. ISBN: 978-14-666-6269-8.

RAVENDA Zbyněk, Martin MANDAL, Jan KODERA a kol. 2012. *Peněžní ekonomie a bankovnictví.* 5. aktualiz. vyd. Praha : Management press, 2012. ISBN: 978-80-7261-279-6.

SCHLOSSBERGER, Otakar a Marcela SOLDÁNOVÁ. 2005. *Platební styk.* 3.,přeprac. a dopl. vyd. Praha : Bankovní institut, a.s., 2005. ISBN: 80-7265-072-6.

SCHLOSSBERGER, Otakar. 2012. *Platební služby.* 1. vyd. Praha : Management press, 2012. ISBN: 978-80-7261-238-3.

Internetové zdroje a elektonická média

Aktuálně. 2015. Hrozí útok na internetové bankovnictví? Expert odpovídal. *Aktuálně.cz.* [Online] Economia, a.s., 2015. [Citace: 14. 07 2016.] https://zpravy.aktualne.cz/finance/hrozi-utok-na-internetove-bankovnictvi-ptejte-se-experta/r~c4d410e0f3cd11e499590025900fea04/.

Axis Communications AB. 2013. Zvýšená bezpečnost a zdokonalené funkce pro bankomaty. *axis.com.* [Online] Axis Communications AB, 2013. [Citace: 07. 11 2016.] http://www.axis.com/files/brochure/bc_atm_surv_54374_cs_1310_lo.pdf.

Bankovnípoplatky. 2010. Zapomenuté peníze v bankomatu? Jinde než v přístroji ČSOB o ně přijdete. *Bankovnípoplatky.com.* [Online] 2010. [Citace: 07. 11 2016.] http://www.bankovnipoplatky.com/2-dil-vraci-se-do-bankomatu-zapomenuta-hotovost-jak-kde-12320.html.

Bezpečnýinternet. 2016. Bezpečně převádět peníze. *Bezpečný internet.cz.* [Online] Česká spořitelna a.s., Microsoft s.r.o.,Seznam.cz a.s., 2016. [Citace: 31. 05 2106.] http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/bezpecne-prevadet-penize.aspx.

Bezpečnýinternet. 2016. Bezpečně se přihlásit. *Bezpečný internet.cz.* [Online] 2016. [Citace: 31. 05 2016.] http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/bezpecne-se-prihlasit.aspx.

Bezpečnýinternet. 2016. Bezpečnost internetového bankovnictví obecně. *bezpečný internet.cz.* [Online] 2016. [Citace: 31. 05 2016.] http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/bezpecnost.aspx.

Bezpečnýinternet. 2016. Vyšší typy zabezpečení. *Bezpečný internet.cz.* [Online] Česká spořitelna a.s., Microsoft s.r.o.,Seznam.cz a.s., 2016. [Citace: 31. 05 2016.] http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/vyssi-typy-zabezpeceni.aspx.

Bezpečnýinternet. 2016. Platím kartou. *bezpecnyinternet.cz.* [Online] Česká spořitelna a.s., Microsoft s.r.o.,Seznam.cz a.s., 2016. [Citace: 11. 07 2016.] http://www.bezpecnyinternet.cz/pokrocily/nakupovani-pres-internet/platim-kartou.aspx.

ČERVINKA, Michal a Pavel SEHNAL. 2003. Silná místa silné autentizace. *Arowecs.cz.* [Online] 2003. [Citace: 04. 10 2016.] http://www.arrowecs.cz/web/read_me.nsf/4f4b7d31e38afd2bc1256cac00352bd3/8fe51bd9a69aa705c1256d49002ffdd2?OpenDocument.

Česká národní banka. 2016. Vybrané předpisy vztahující se k platebnímu styku. *cnb.cz.* [Online] 2016. [Citace: 28. 12 2016.] http://www.cnb.cz/cs/platebni_styk/pravni_predpisy/index.html.

Česká národní banka. 2015. Výroční zpráva.*cnb.cz.* [Online] 2015. [Citace: 08. 11 2016.] https://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/o_cnb/hospodareni/vyrocni_zpravy/download/vyrocni_zprava_2015.pdf. ISBN: 978-80-87225-62-2.

Česká spořitelna, a.s. 2016. SERVIS 24 Internetbanking - zabezpečení. *csas.cz.* [Online] Česká spořitelna a.s., 2016. [Citace: 01. 06 2016.] http://www.csas.cz/banka/nav/osobni-finance/servis-24---internetbanking/zabezpeceni-d00020048.

Československá obchodní banka, a.s. 2016. Obchodní podmínky pro elektronické bankovnictví a elektronickou komunikaci Poštovní spořitelny. *Erasvet.* [Online] 2016. [Citace: 04. 11 2016.] https://www.erasvet.cz/documents/296002/297359/ALL-podminky-elektronickeho-bankovnictvi.pdf. ISSN: 2464-4579.

EMVCo. 2016. EMV Connection. *EMV Chip Payment Technology: Frequently Asked Questions.* [Online] 2016. [Citace: 26. 10 2016.] http://www.emv-connection.com/emv-faq/ .

Erasvet. 2012. *erasvet.cz.* [Online] Československá obchodní banka,a.s., 2012. [Citace: 26. 10 2016.] https://www.erasvet.cz/fyzicke-osoby/ostatni/stranky/platebni-karty/bezpecne-platby-na-internetu.aspx#1.

GAŠPARÍK, Petr. 2015. Vícefaktorová autentitace: Jak vypadá praxe? *computerworld.cz.* [Online] 2015. [Citace: 27. 09 2016.] http://computerworld.cz/securityworld/vicefaktorova-autentizace-jak-vypada-praxe-51923.

KLUFA František, Petr SCHOLZ a Michaela KOZKOVÁ. 2009. Podvody v oblasti bezhotovostních plateb v ČR (studie). *Finarbitr.* [Online] 2009. [Citace: 12. 10 2016.] http://www.finarbitr.cz/download/137_cs_a5_bezhotovostni_podvody.pdf.

Komerční banka a.s. 2016. www.kb.cz. *Základní informace o platebních kartách.* [Online] 2016. [Citace: 11. 07 2016.] http://www.kbkarty.cz/cs/platebni-karty/zakladni-informace/.

LOUDA, Pavel. 2016. Jaká je budoucnost v oblasti bezpečnosti? *computerworld.cz.* [Online] IDG Czech Republic, a. s. , 2016. [Citace: 27. 09 2016.] http://computerworld.cz/securityworld/jaka-je-budoucnost-v-oblasti-bezpecnosti-52674.

MoneyMAG. 2016. Fiobanka zvyšuje bezpečnost platebních karet. *MoneyMAG.cz.* [Online] ICORP a.s., 2016. [Citace: 30. 11 2016.] http://moneymag.cz/bankovnictvi/7252-fio-banka-zvysuje-bezpecnost-platebnich-karet. ISSN: 2336-2588.

NĚMEC, Dalibor. 2008. Bezpečnost platebních systémů: mýty a skutečnost. *bankovnipoplatky.com.* [Online] 2008. [Citace: 14. 12 2016.] http://www.bankovnipoplatky.com/bezpecnost-platebnich-systemu-myty-a-skutecnost-4433.html.

Platební terminály. 2016. Platební terminály ČR. *terminalzdarma.cz.* [Online] KAM MEDIA s.r.o., 2016. [Citace: 17. 10 2016.] http://www.terminalzdarma.cz/.

Policie ČR. 2016. SKIMMING. *policie.cz.* [Online] 2016. [Citace: 23. 11 2016.] http://www.policie.cz/clanek/skimming-2013.aspx.

Policie ČR. 2016. Statistiky kriminality. *policie.cz.* [Online] 12. 09 2016. http://www.policie.cz/statistiky-kriminalita.aspx.

PŘIBYL, Tomáš. 2015. Computerworld. *SecurityWorld.* [Online] IDG Czech Repoblic, a.s.,06.06.2015.[Citace:29.09.2016.]http://computerworld.cz/securityworld/nezapominejte-na-fyzickou-bezpecnost-52097.

Computerworld. 2015. Nezapomínejte na fyzickou bezpečnost. *computerworld.cz.* [Online] 2015. [Citace: 27. 09 2016.] http://computerworld.cz/securityworld/nezapominejte-na-fyzickou-bezpecnost-52097.

PULTZNER, Martin. Češi chtějí platit mobilem a otiskem prstu. *nearfield.cz.* [Online] [Citace: 26. 10 2016.] https://nearfield.cz/clanky/cesi-chteji-platit-mobilem-a-otiskem-prstu-vyslo-z-vyzkumu-mastercardu-200.

Raiffeisenbank. 2016. Bezpečnost internetového bankovnictví. *rb.cz.* [Online] Raiffeisenbank a.s., 2016. [Citace: 01. 06 2016.] https://www.rb.cz/informacni-servis/doplnkove-informace-k-produktum/bezpecne-bankovnictvi/bezpecnost-internetoveho-bankovnictvi.

Sdružení pro bankovní karty. 2016. Statistiky SBK. *bankovnikarty.cz.* [Online] 2016. [Citace: 11. 07 2016.] http://www.bankovnikarty.cz/pages/czech/profil_statistiky.html.

ŠNAJDR, Petr. 2013. Systemonline.cz. *Dvoufaktorová autentizace: mýty a realita.* [Online] 2013. [Citace: 03. 10 2016.] http://www.systemonline.cz/it-security/dvoufaktorova-autentizace-myty-a-realita.htm . ISSN: 1802-615X.

ŠNAJDR, Petr. 2013. Systemonline.cz. *IT SYSTEMS.* [Online] CCB, s.r.o., 06 2013. [Citace: 03. 10 2016.] https://www.systemonline.cz/it-security/dvoufaktorova-autentizace-myty-a-realita.htm. ISSN 1802-615X.

TERRA-KLUB, o.p.s. Terra-klub.cz. *Jak postupovat při výběru hotovosti z bankomatu?* [Online] 2016. [Citace: 12. 09 2016.] http://www.terra-klub.cz/cs/.

UniCreditBank. 2016. Přijímání platebních karet. *unicreditbank.cz.* [Online] UniCredit Bank Czech Republic and Slovakia,a.s., 2016. [Citace: 26. 10 2016.] https://www.unicreditbank.cz/content/dam/cee2020-pws-cz/cz-dokumenty/POP_P%C5%99ij%C3%ADm%C3%A1n%C3%AD%20platebn%C3%ADch%20karet.pdf.

WEBSTER, Karen. 2016. PYMNTS.com. *Securrity and risk.* [Online] 2016. [Citace: 26. 10 2016.] http://www.pymnts.com/news/security-and-risk/2016/digital-identity-trends/.

ZUNO BANK AG. 2016. Bezpečnost je pro nás důležitá. *zuno.cz.* [Online] Raiffeisenbank a.s., 2016. [Citace: 13. 09 2016.] https://www.zuno.cz/pomoc/bezpecnost/online-banking/.

8 Přílohy

Příloha č.1 Dotazník

Příloha č.1

Dotazník k bezhotovostnímu platebnímu styku

Dobrý den,

jmenuji se Aleš Podaný a jsem studentem Provozně ekonomické fakulty České zemědělské univerzity v Praze. Tento dotazník je určen k šetření v rámci diplomové práce na téma „**Bezhotovostní platební styk“,** která je řešena v rámci mého studia. Zajímají mě Vaše zkušenosti a hodnocení, z tohoto důvodu si Vás dovoluji požádat o vyplnění dotazníku, který je anonymní. Výstupy tohoto dotazníkového šetření budou využity pro vypracování mé diplomové práce.

Děkuji.

Odpovědi označte křížkem v symbolu čtverečku.

Otázky.

1. Uveďte pohlaví:

☐ muž ☐ žena

2. Vaše věková kategorie?

☐ 18-30 let ☐ 31-40 let ☐ 41-50 let ☐ 50- 60 let ☐ 60 a více let

3. Jaké je Vaše nejvyšší dosažené vzdělání?

☐ základní ☐ střední ☐ úplné střední (s maturitou) ☐ vyšší odborné ☐ vysokoškolské

4. Máte zřízen běžný účet?

☐ ano ☐ ne

5. Jste uživatelem internetového bankovnictví?

☐ ano ☐ ne

(pokud byla Vaše odpověď „**ne**” pokračujte otázkou č. 13)

6. Jak často používáte internetové bankovnictví

☐ ojediněle ☐ občas ☐ často ☐ velmi často

7. Pro přihlášení do internetového bankovnictví používáte autorizační sms zprávy?

☐ ano ☐ ne

8. Prostřednictvím kterého z uvedených zařízení se přihlašujete k internetovému bankovnictví?

☐ telefon ☐ tablet ☐ osobní počítač ☐ notebook ☐ jiné, uveďte …….

(zde může být více odpovědí)

9. Používáte ve svém zařízení pro přístup k internetovému bankovnictví, jako zabezpečení, některý z uvedených programů?

☐ antivirový program ☐ antispyware (protišpionážní program) ☐ nepoužívám program pro zabezpečení ☐ jiný program, uveďte…….

10. Připojil/a jste se někdy k internetovému bankovnictví prostřednictvím veřejné wi-fi sítě?

☐ ano ☐ ne

11. Máte aktivovány sms zprávy o pohybech na účtu?

☐ ano ☐ ne

12. Hesla pro přihlášení do bankovnictví máte nějakým způsobem zabezpečená?

☐ ano ☐ ne

(např. trezor, aplikace, token, atd.)

13. Jste držitelem platební karty?

☐ ano ☐ ne

(pokud byla Vaše odpověď „**ne**" pokračujte otázkou č. 20)

14. Kterým z níže uvedených prvků je Vaše platební karta opatřena?

☐ magnetický proužek ☐ čip ☐ bezkontaktní čip ☐ hologram ☐ jiné, uveďte ……

(zde může být více odpovědí)

15. Při zadávání PINu na platebním terminálu obchodníka zakrýváte číselník PIN padu?

☐ ano ☐ ne

16. Při zadávání PINu u bankomatu zakrýváte číselník?

☐ ano ☐ ne

17. Nosíte u sebe zapsaný PIN platební karty?

☐ ano ☐ ne

18. Máte aktivovány sms zprávy o provedených platbách?

☐ ano ☐ ne

19. Pro výběr hotovosti používáte bankomat

☐ pouze své banky ☐ převážně své banky ☐ převážně ostatních bank ☐ bankomat nepoužívám

20. Víte, co znamená pojem phishing?

☐ ano ☐ ne

21. Víte, co znamená pojem pharming?

☐ ano ☐ ne

22. Setkal/a jste se ve svém bezprostředním okolí s podvodným jednáním, v oblasti platebních karet nebo elektronického bankovnictví?

☐ ano ☐ ne

Zde můžete uvést své návrhy opatření, nebo vylepšení, které zvýší úroveň bezpečnosti internetového bankovnictví a platebních karet.

……

……

……
